High-Power Wireless 150N Outdoor CPE / Access Point

User Manual

Model 525794

INTELLINET®
NETWORK SOLUTIONS

INT-525794-UM-0715-01

TABLE OF CONTENTS

Introduction 3
Package Contents 3
Product Features 3
Product Specifications 4
Hardware 4
Device Status LEDs 4
Connectors 5
Passive-PoE Injector 5
Connecting the device to the network 6
Configuring the device 7
Accessing the web configuration interface 7
Setup Wizard 8
Operation Modes – When to use which 11
Router (Gateway) 11
WISP-Wireless ISP 12
Access Point 13
Repeater 14
Status 15
Wireless Settings 16
Basic 16
M-SSID 16
ACL 16
WDS 17
WMM 19
Advanced 20
Network 23
Network Settings in Router Mode 23
Network Settings in WISP Mode 26
Network Settings in Access Point (AP) Mode 27
Network Settings in Repeater Mode 28
QoS (in Router and WISP Mode) 29
Security (in Router and WISP Mode) 32
IP/Port Filter: 33
URL Filtering: 33
MAC Filtering: 33
DoS Protection: 34
System 35
Password Settings 35
Time Settings 35
Backup & Restore 35
Factory Defaults 36
Reboot 36
Smart Reboot 36
Web Server 37
Firmware Upgrade 37
Debug Tools 38
Log Settings 38
Ping Test 38
Appendix A: Changing the IP Address of a Network Adapter 39
Appendix B: Troubleshooting 44
Appendix C: DSCP Value Table 45
Appendix D: Warranty Information 46

INTRODUCTION

The Intellinet High-Power Wireless 150N Outdoor CPE Access Point, Model 525794, is a cost-effective WISP CPE (customer-premises equipment) and long-distance wireless bridge solution. It combines the functionality of a classic wireless access point, a wireless ISP (WISP) client, a 10 dBi high-gain antenna and an IP65 weatherproof enclosure. High output power (up to 4 watts in FCC-regulated countries) and high receiver sensitivity significantly extend the transmission range, making the Intellinet 525794 Wireless CPE an excellent choice for point-to-point wireless connections.

The High-Power Wireless 150N Outdoor CPE / Access Point provides maximum wireless security by supporting 802.1x user authentication for external RADIUS servers. Other security features included in this access point are MAC address filtering, disable SSID broadcast and support for the latest wireless encryption mechanisms.

PACKAGE CONTENTS

Ensure that the following items are included:

- High-Power Wireless 150N Outdoor CPE / Access Point
- Quick installation guide
- Installation CD with user manual (this document)
- Passive PoE power adapter
- Pole mount clamp

PRODUCT FEATURES

- Wireless outdoor CPE provides Internet connectivity to your 2.4 GHz Wireless ISP (WISP)
- Also suitable for long-range PtP bridge connections
- Built-in 10 dBi antenna
- Weatherproof and corrosion resistant, IP65
- Supported modes: Router (Gateway), Access Point, AP Client, WISP and WDS Bridge
- Complies with 2.4 GHz IEEE 802.11n standard and is backward compatible with IEEE 802.11g/b standards
- Supports WEP and WPA/WPA2 (TKIP and AES) data encryption
- Supports multiple ESSIDs with individual security settings
- Supports VPN pass-through for L2TP, IPsec and PPTP connections
- Up to 150 Mbps network link speed
- SMA connector for optional external antenna
- LNA (Low Noise Amplifier) technology for improved radio performance
- Included passive POE injector for up to 60 meters (200 feet) connection distance

PRODUCT SPECIFICATIONS

Standards

- IEEE 802.11b (11 Mbps Wireless LAN)
- IEEE 802.11g (54 Mbps Wireless LAN)
- IEEE 802.11n (150 Mbps Wireless LAN)
- IEEE 802.1x (Network Access Control)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3u (100Base-TX Fast Ethernet)

Wireless

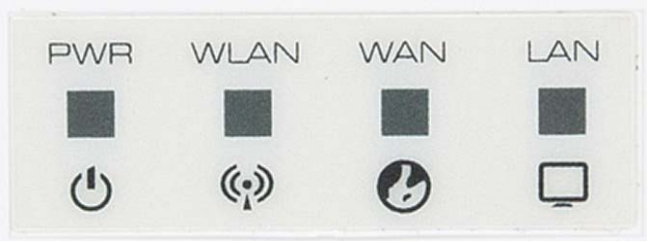
- Wireless frequency range: 2.400 – 2.484 GHz
- EIRP Output power EU (ETSI): 20 dBm
- EIRP Output power U.S. (FCC): 36 dBm
- Wireless channels EU (ETSI): 1-13, US (FCC): 1-11

Power

- External power adapter: 12 V DC, 1.0 A

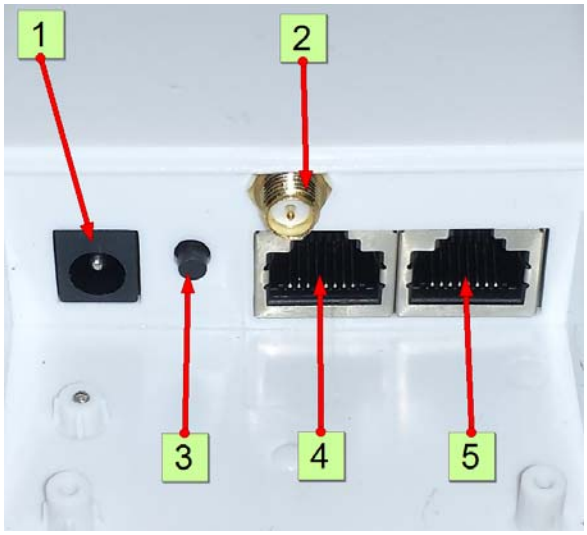
HARDWARE

DEVICE STATUS LEDS



LED Indicator	State	Description
PWR	On	The Intellinet CPE Access Point is turned on.
	Off	The Intellinet CPE Access Point is turned off.
WLAN	On	The wireless radio is active.
	Off	The wireless radio is inactive.
	Flashing	The wireless radio is active, and data is being transmitted and received.
WAN	On	Link on WAN port is active.
	Off	Link on WAN port is inactive.
	Flashing	Link on WAN port is active, and data is being transmitted and received.
LAN	On	Link on LAN port is active.
	Off	Link on LAN port is inactive.
	Flashing	Link on LAN port is active, and data is being transmitted and received.

CONNECTORS

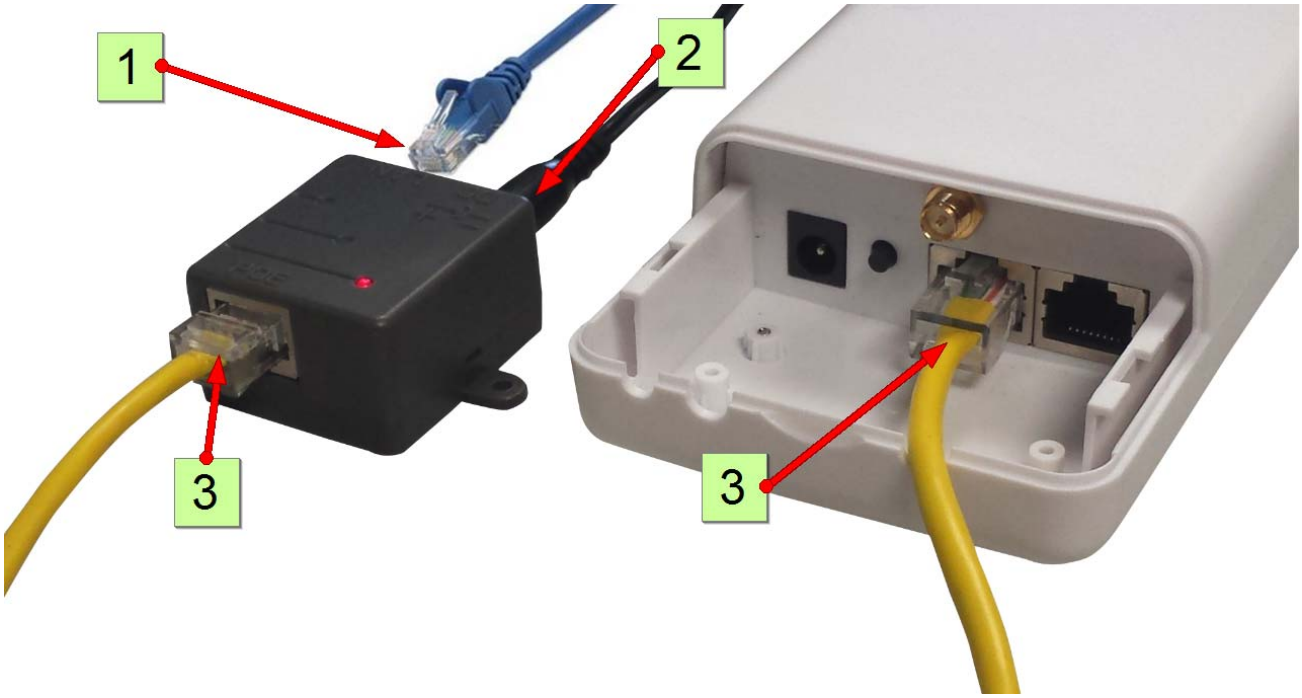


Item	Description
1	Connection for external power adapter (12 V DC, 1.0 A). Use this, if you do not want to utilize the included Passive-PoE injector.
2	Female RP-SMA connector for the connection of an external high-gain antenna.
3	Reset button. Depress for 10 seconds to initiate a reset to factory default values.
4	LAN connector and passive-PoE input port. This port needs to be connected to your local network via a RJ45 cable, if you use the Intellinet CPE Access Point as a regular access point or repeater
5	Optional WAN connector. This needs to be used if you run the Intellinet CPE Access Point in router/gateway mode. In that scenario, the WAN port must be connected to a port that provides Internet access, i.e., the LAN port on the cable modem.

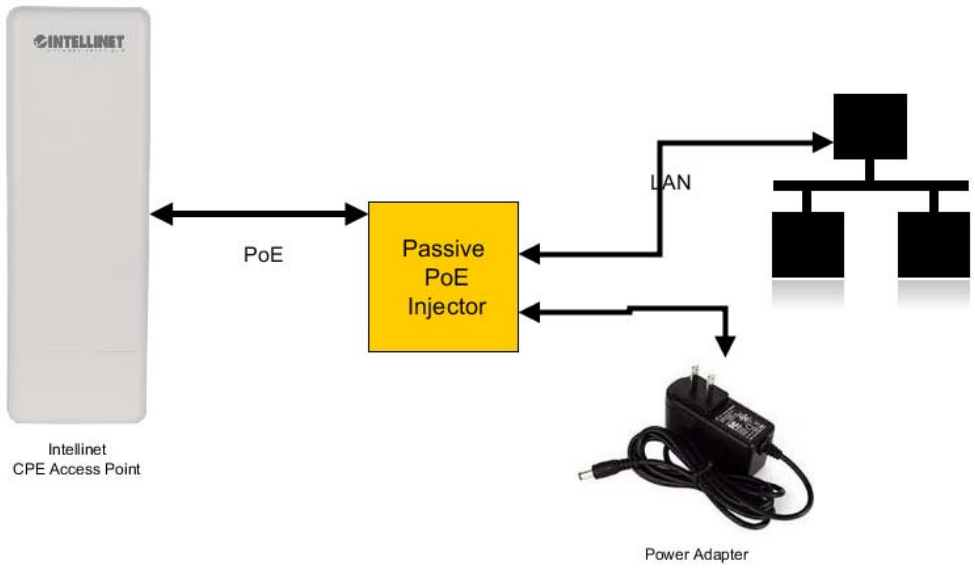
PASSIVE-POE INJECTOR

The Intellinet CPE Access Point comes with a Passive-PoE Injector that enables to merge the power supply and data to one Ethernet cable and supply them to the access points with PoE input (LAN) port. It has three connection points. A power input port for the external 12 V DC power adapter, a LAN port for the connection to your local network, and a PoE port for the connection to the access point's LAN port.

CONNECTING THE DEVICE TO THE NETWORK



Item	Description
1	Connect the external power adapter (12 V DC, 1.0 A) to a power outlet, and to the Passive-PoE injector. Once the connection is made, the power LED on the PoE injector will light up.
2	Connect a standard RJ45 Ethernet cable to the LAN port on the Passive-PoE Injector. That cable connects the PoE injector (and thus the access point) to the rest of your network.
3	Connect a standard RJ45 Ethernet cable (8P8C) from the PoE port of the Passive-PoE Injector to the LAN port of the Intellinet CPE Access Point. This connection provides power and data connectivity to the access point.

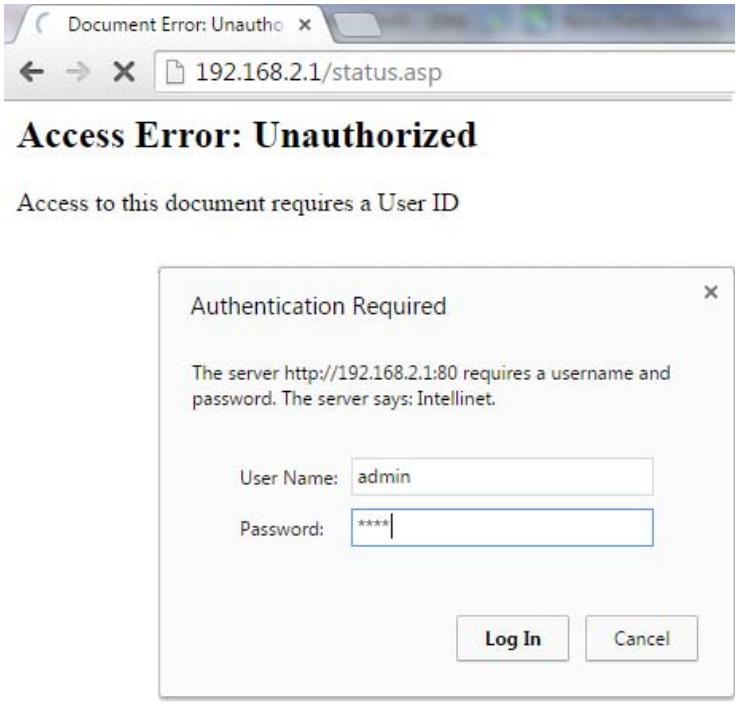


CONFIGURING THE DEVICE

ACCESSING THE WEB CONFIGURATION INTERFACE

The Intellinet CPE Access Point is equipped with an array of features, which can be configured to your needs. Configuration is done by means of a standard web browser. Open http://192.168.2.1 in your Web browser, and then type in admin as the user name and 1234 as the password. Click **Log In** to connect.

Default IP address: 192.138.2.1
Default IP subnet mask: 255.255.255.0
User name: admin
Password: 1234

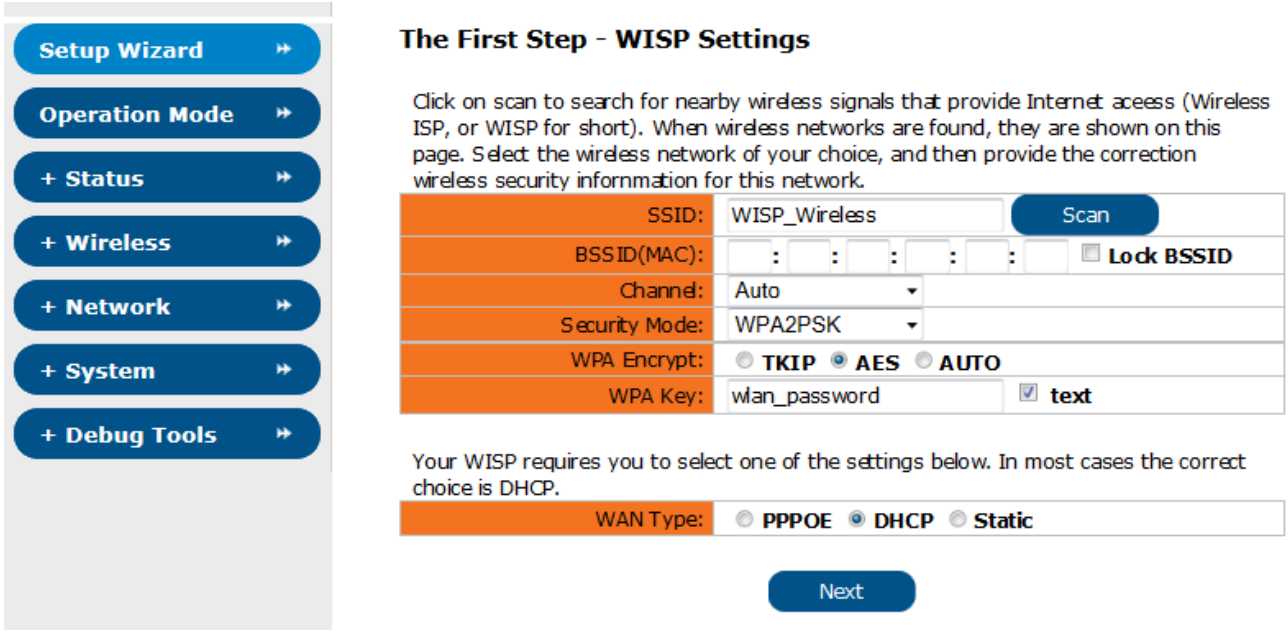


Should you encounter problems connecting to the web interface of the access point, one of the following issues may be occurring.

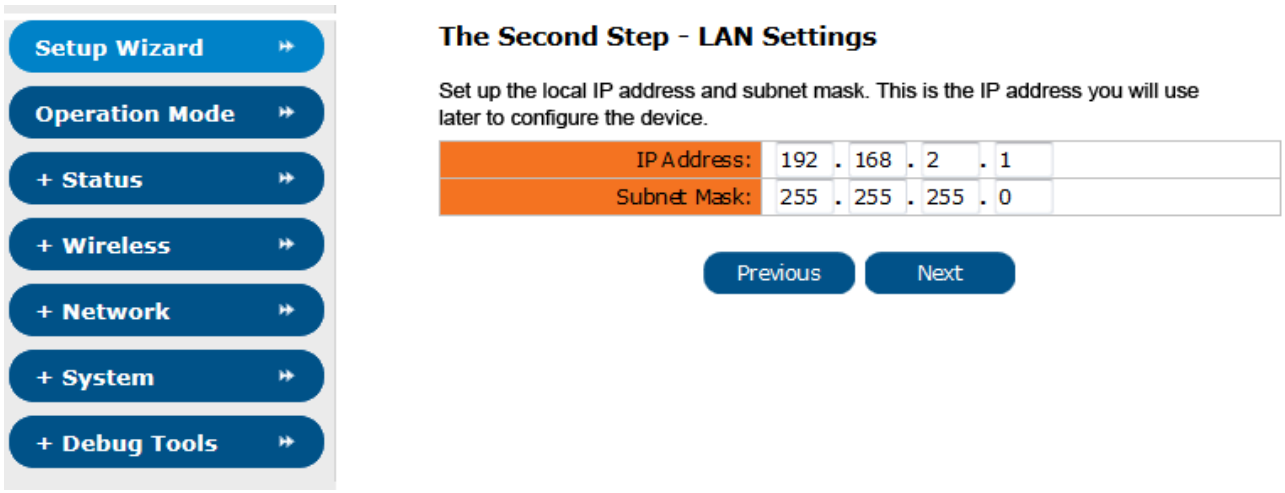
- Your computer's IP address is not compatible to the IP address of the Intellinet CPE Access Point. It must be in range of 192.168.2.2 to 192.168.2.254.
  Refer to Appendix A for information on how to set up the IP address of the network adapter.
- The Intellinet CPE Access Point isn't properly connected to either the LAN port of your computer, or the network. Verify that the LAN status LED is lit.
- The IP address of your Intellinet CPE Access Point may have been changed. To ve certain, a hardware reset should be performed. To do that, simply press the reset button for 10 seconds while the device is powered up.

SETUP WIZARD

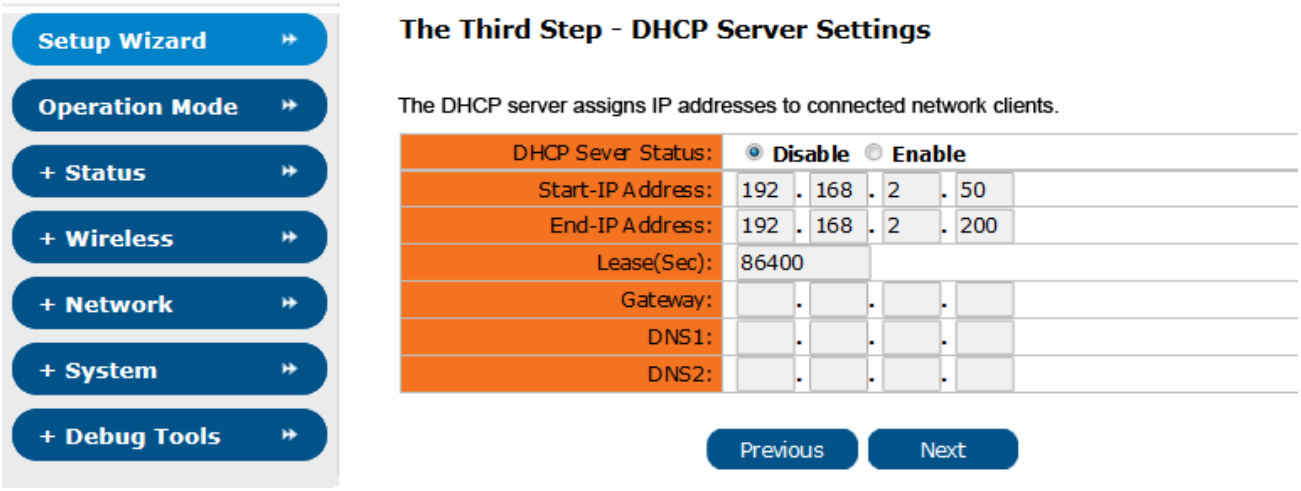
The setup wizard should only be used, if you want to set up the Intellinet CPE Access Point as a CPE for a wireless ISP. All other operational modes are set up without the use of the setup wizard. For a description of the operational modes, refer to the next section.


Setup Wizard
Operation Mode
+ Status
+ Wireless
+ Network
+ System
+ Debug Tools
The First Step - WISP Settings
Click on scan to search for nearby wireless signals that provide Internet aceess (Wireless ISP, or WISP for short). When wireless networks are found, they are shown on this page. Select the wireless network of your choice, and then provide the correction wireless security infornmation for this network.
SSID: WISP_Wireless Scan
BSSID(MAC): Lock BSSID
Channel: Auto
Security Mode: WPA2PSK
WPA Encrypt: TKIP AES AUTO
WPA Key: wlan_password text
Your WISP requires you to select one of the settings below. In most cases the correct choice is DHCP.
WAN Type: PPPOE DHCP Static
Next

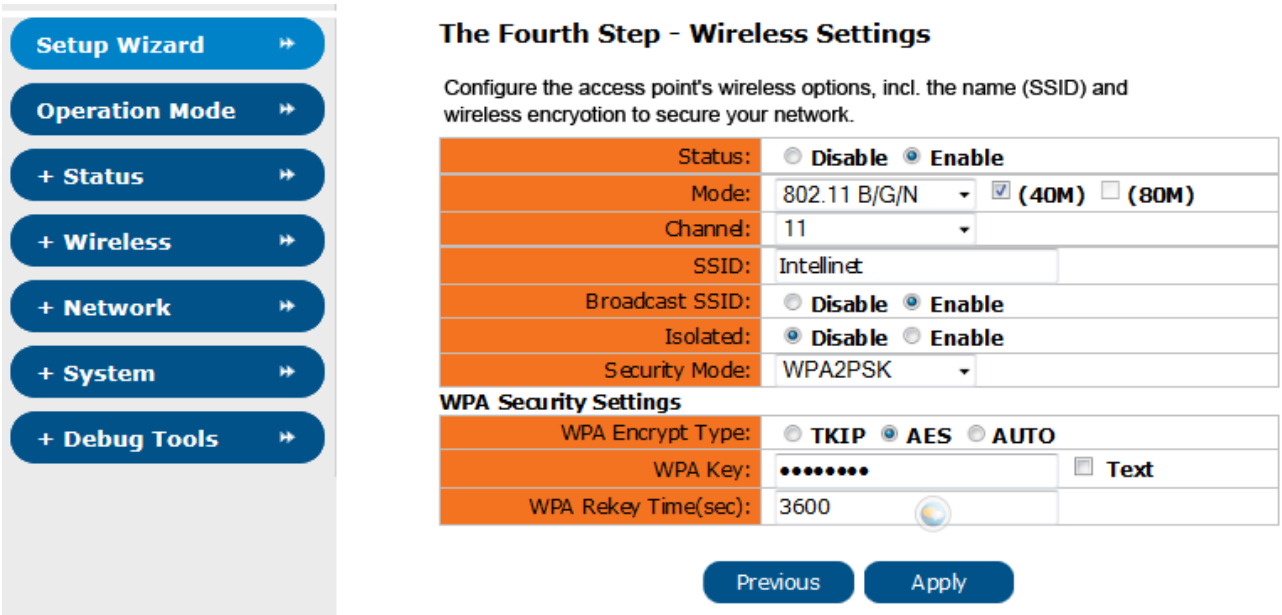
On the first screen of the setup wizard you need to define which wireless signal you want to connect to. That signal should be the wireless signal of your wireless ISP. Click on **Scan** to display of a list of all available wireless networks, select the network of your WISP, and then type in the password required for the WISP in the **WPA Key** field.
You also need to select the **WAN Type** that is compatible to the settings of your WISP.


Setup Wizard
Operation Mode
+ Status
+ Wireless
+ Network
+ System
+ Debug Tools
The Second Step - LAN Settings
Set up the local IP address and subnet mask. This is the IP address you will use later to configure the device.
IP Address: 192 . 168 . 2 . 1
Subnet Mask: 255 . 255 . 255 . 0
Previous
Next

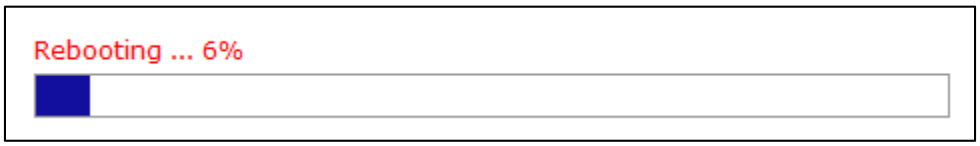
The second screen allows you to define the device IP address of the Intellinet CPE Access Point. The default value is 192.168.2.1.



The third setup wizard screen deals with the DHCP server function of the Intellinet CPE Access Point. Whether or not you will need to use this, will depend on your WISP. However, it is more likely than not, that the DHCP server should be disabled. If you do need to enable the DHCP server, then you will need to fill out the IP address related fields.

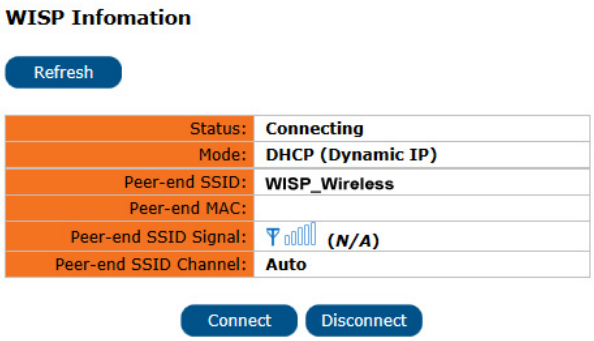


Screen number four lets you set up wireless service for your local clients. If you disable it, then Internet service will only be available to clients that are connected to the LAN port of the access point, either directly, or indirectly via a switch. If you enable the wireless function, then you need to define the usual wireless parameters, such as the SSID and the security settings.

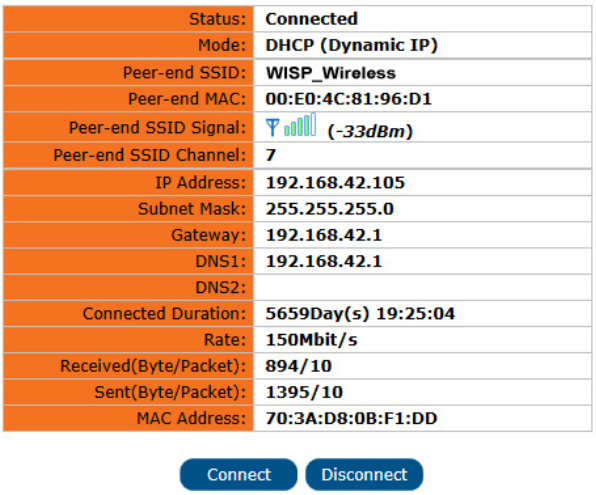


Click **Apply** to save the settings and reboot the access point.

Once the reboot is completed, the Intellinet CPE Access Point will try to establish a connection with the WISP signal, indicated by the status **Connecting**. Click Refresh after about 30 seconds and the status will have changed to **Connected**.



This screen provides detailed information about the connection to the WISP signal, and it allows to **Disconnect** and **Reconnect** the WISP signal using the corresponding buttons.

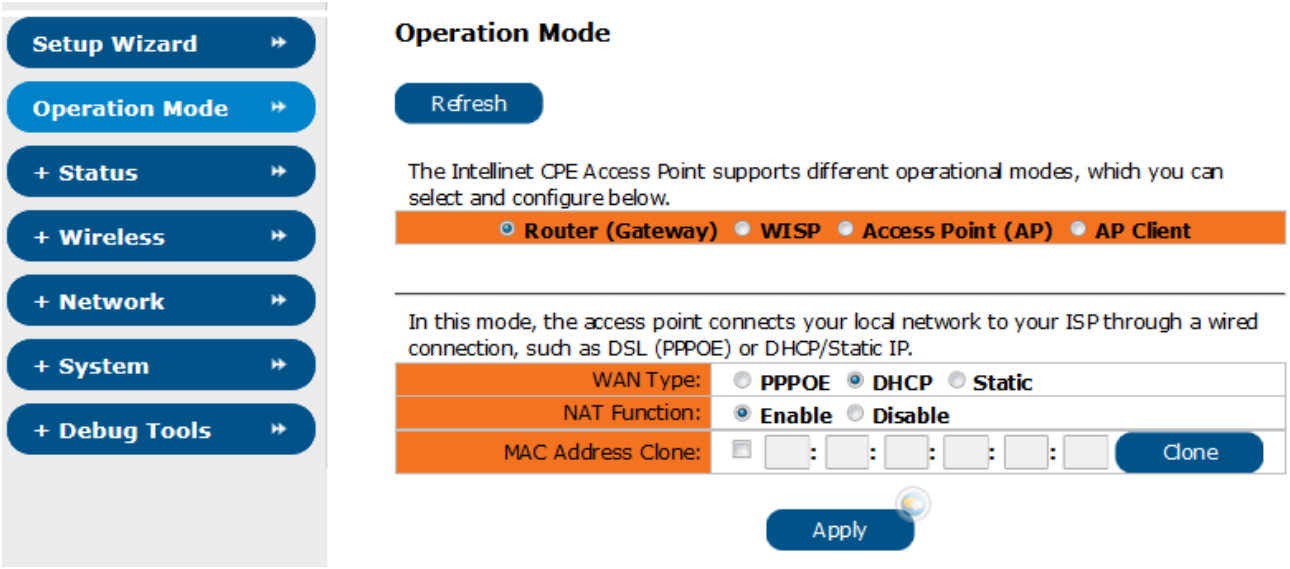


OPERATION MODES – WHEN TO USE WHICH

Your Intellinet CPE Access Point supports 4 operation modes: Router (Gateway), WISP, Access Point (AP) and Repeater. Before you start making changes to the configuration, you should familiarize yourself with these modes.

ROUTER (GATEWAY)

A router connects multiple local network clients to one Internet connection, and provides basic NAT firewall protection at the same time. Use this mode if you want the Intellinet CPE Access Point to function as the (wireless) router in your network. If you choose this mode, you must connect the WAN port of the access point to a network port that provides Internet connection, such as a DSL or cable modem.

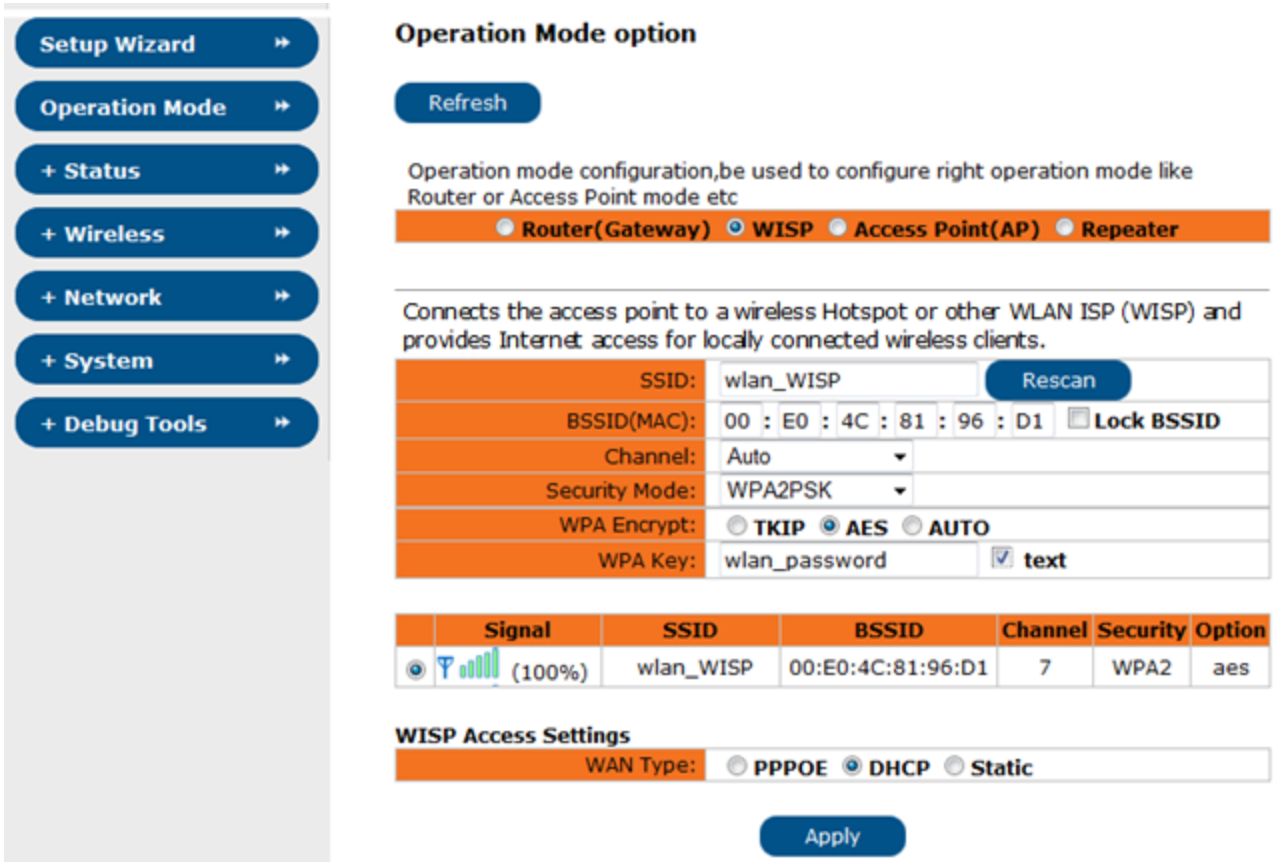


Select the correct WAN type for your ISP, e.g., PPPOE for xDSL connections, or DHCP for cable Internet service. If you select PPPOE, you must provide the username and password, as well as advanced parameters such as MTU, LCP echo interval and failure. Your DSL service provide has this information. If your Internet service uses static IP, you'll need to enter the IP address and related information into the configuration interface. In many cases, however, your Internet access is established by means of DHCP. In this case there is nothing to configure but the optional cloned MAC address, which you only need to enter if your Internet service requires a certain MAC address.

The NAT function should be enabled, as it provides the basic router and firewall functionality you would expect from a router.

WISP-WIRELESS ISP

A wireless Internet service provider (WISP) is an Internet service provider with a network based on wireless networking. If you live in an area where Internet service is provided by a 2.4 GHz Wireless IEEE 802.11n signal, you can utilize the Intellinet Access Point as a CPE (Customer-premises equipment). When you activate WISP mode, you will need to specify the SSID of the WISP signal, along with the security settings if so required. You also need to define how the connection to the WISP is established, i.e., DHCP, PPPoE, etc. After the obligatory reboot, the Intellinet CPE wirelessly connects to the WISP, and also provides local wireless access in your network.

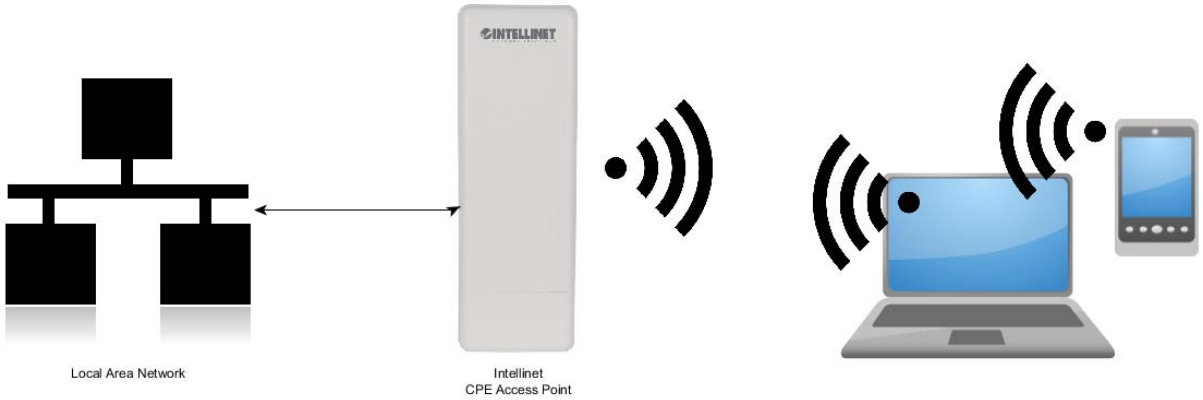

Setup Wizard
Operation Mode
+ Status
+ Wireless
+ Network
+ System
+ Debug Tools
Operation Mode option
Refresh
Operation mode configuration,be used to configure right operation mode like Router or Access Point mode etc
Router(Gateway) WISP Access Point(AP) Repeater
Connects the access point to a wireless Hotspot or other WLAN ISP (WISP) and provides Internet access for locally connected wireless clients.
SSID: wlan_WISP Rescan
BSSID(MAC): 00 : E0 : 4C : 81 : 96 : D1 Lock BSSID
Channel: Auto
Security Mode: WPA2PSK
WPA Encrypt: TKIP AES AUTO
WPA Key: wlan_password text
Signal SSID BSSID Channel Security Option
(100%) wlan_WISP 00:E0:4C:81:96:D1 7 WPA2 aes
WISP Access Settings
WAN Type: PPPOE DHCP Static
Apply

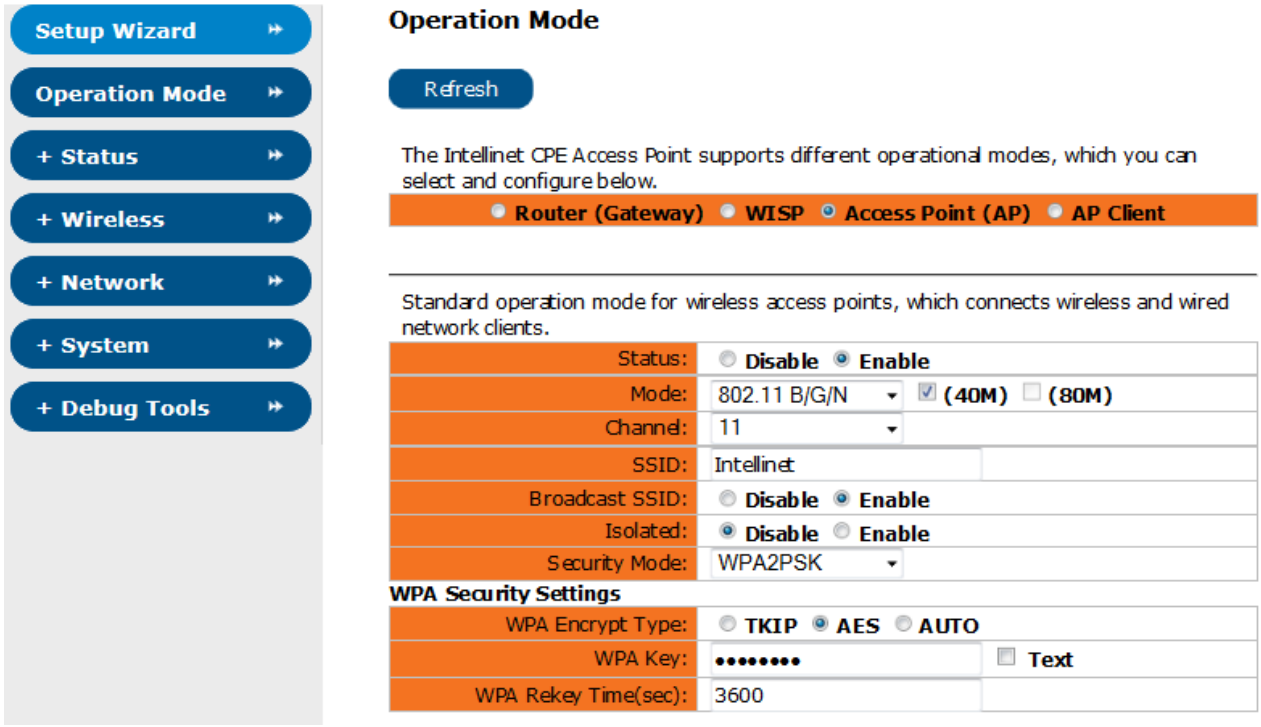
Click on **Scan** to search for available wireless signals in the area. Select the wireless network ("wlan_ISP" in the example above), and the channel, security mode and WLAN Encrypt will be filled out automatically. Type in the password for the wireless network in the field **WPA Key**. Note that this is only required if the WISP signal uses WPA encryption. Should the WISP signal use WEP encryption, the interface presents you with slightly different fields that need to be filled out, namely the WEP key type, key identifier and the actual WEP key fields.

Lock BSSID makes sure that the Intellinet CPE Access Point will always connect to this WISP signal, even if the name of the WISP signal were to ever change.

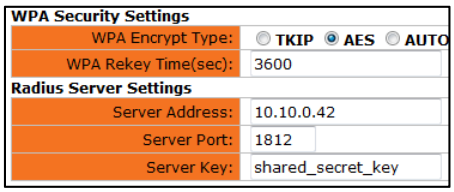
ACCESS POINT

This is the default operation mode of the Intellinet CPE Access Point. A wireless access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi. In this mode, the device acts as a simple network switch connecting wireless and wired network clients.




Setup Wizard
Operation Mode
+ Status
+ Wireless
+ Network
+ System
+ Debug Tools
Operation Mode
Refresh
The Intellinet CPE Access Point supports different operational modes, which you can select and configure below.
Router (Gateway) WISP Access Point (AP) AP Client
Standard operation mode for wireless access points, which connects wireless and wired network clients.
Status: Disable Enable
Mode: 802.11 B/G/N (40M) (80M)
Channel: 11
SSID: Intellinet
Broadcast SSID: Disable Enable
Isolated: Disable Enable
Security Mode: WPA2PSK
WPA Security Settings
WPA Encrypt Type: TKIP AES AUTO
WPA Key: •••••••• Text
WPA Rekey Time(sec): 3600

In order to use the Intellinet CPE as an access point, you need to set the **Status** to **Enable**, set the **Mode** to **11B/G/N** (recommended), set the **Channel** to a value that puts this wireless network at least 4 channels apart from an existing wireless network that might be in close proximity. For example, if another wireless network in range is set to channel 2, then it'd be best to set your Intellinet CPE Access Point to channel 6 or higher. Next, provide the **SSID** and set up the **Security Mode** for the wireless network. **WPA2PSK** is recommended as it provides the most robust security for your wireless network.

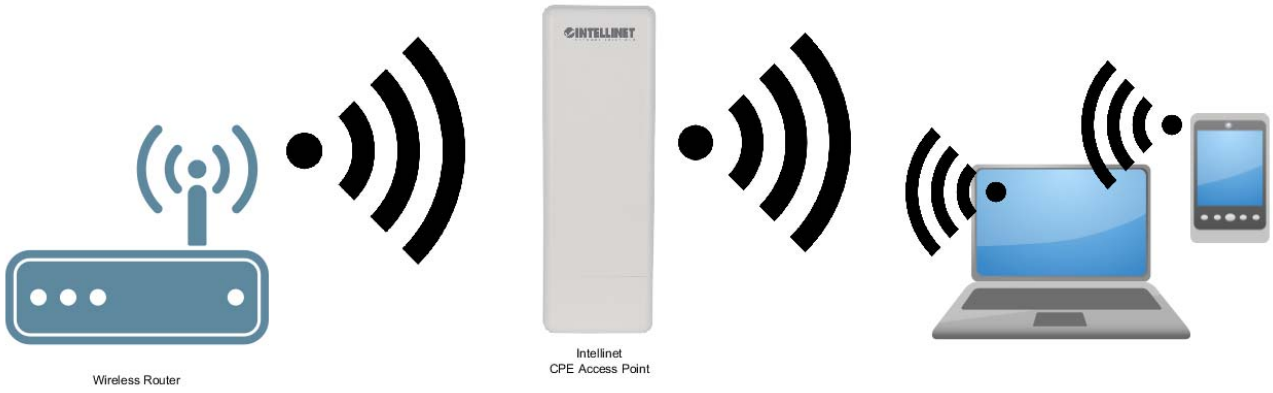


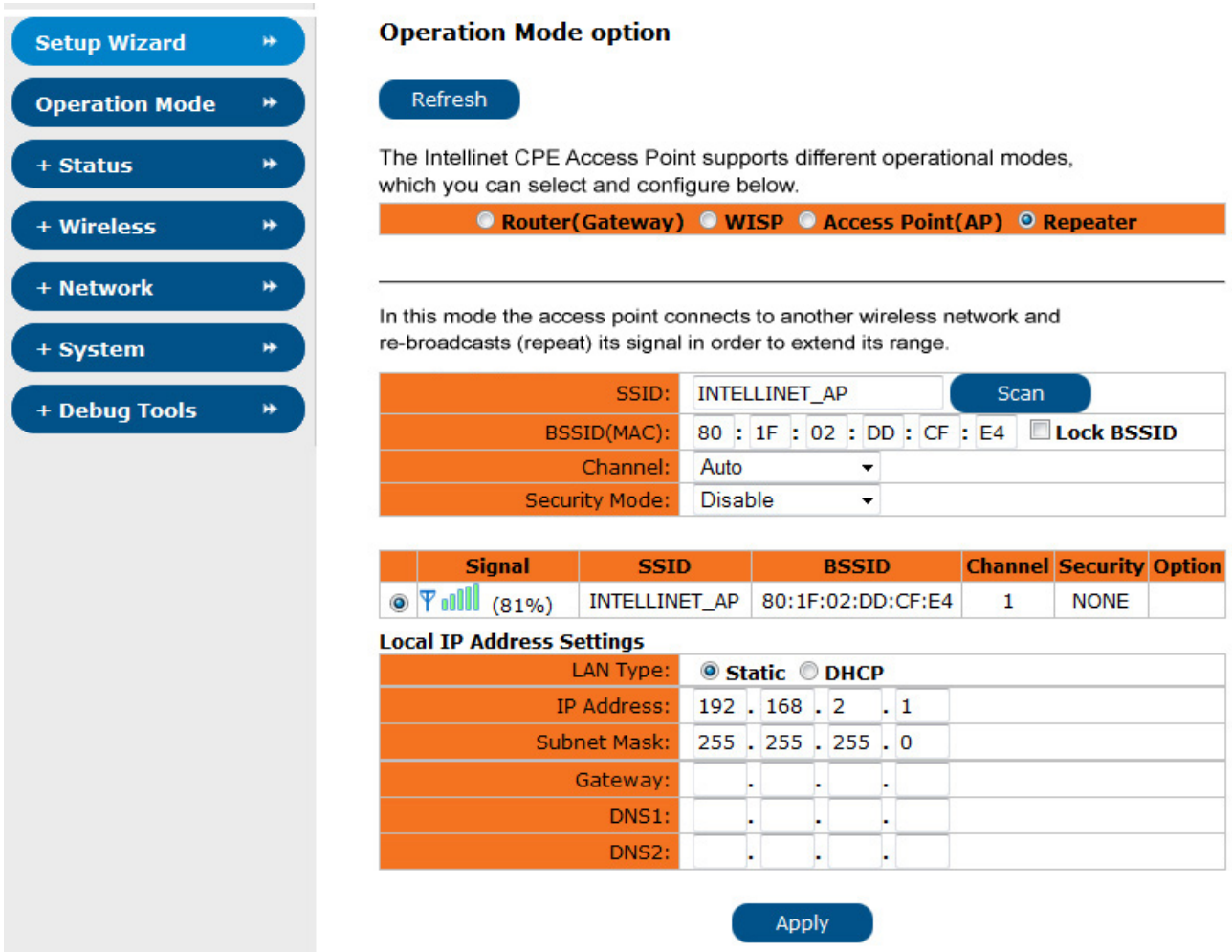
If you use a Radius server in your network to authenticate the wireless clients, you must select Enterprise as the security mode, and again the WPA2 variant is the preferred choice. If you select Enterprise encryption, you must provide the server address, port and shared secret key.

Finally, you must specify the local IP address for your access point. The default address is 192.168.2.1, but you can change it here if you so desire. See next page for further details.

REPEATER

A wireless repeater (also called wireless range extender) takes an existing signal from a wireless router or wireless access point and rebroadcasts it to amplify the wireless signal, extending its range in the process. When you activate this mode, you need to specify the wireless network which you wish to 'repeat', or amplify. After you provide the required security information, the Intellinet CPE Access Point performs a restart.

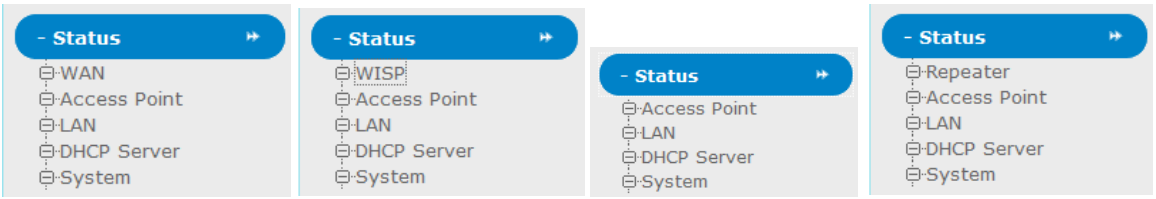



Setup Wizard
Operation Mode
+ Status
+ Wireless
+ Network
+ System
+ Debug Tools
Operation Mode option
Refresh
The Intellinet CPE Access Point supports different operational modes, which you can select and configure below.
Router(Gateway) WISP Access Point(AP) Repeater
In this mode the access point connects to another wireless network and re-broadcasts (repeat) its signal in order to extend its range.
SSID: INTELLINET_AP Scan
BSSID(MAC): 80 : 1F : 02 : DD : CF : E4 Lock BSSID
Channel: Auto
Security Mode: Disable
Signal SSID BSSID Channel Security Option
(81%) INTELLINET_AP 80:1F:02:DD:CF:E4 1 NONE
Local IP Address Settings
LAN Type: Static DHCP
IP Address: 192 . 168 . 2 . 1
Subnet Mask: 255 . 255 . 255 . 0
Gateway:
DNS1:
DNS2:
Apply

The setup is virtually identical to the WISP mode. Click **Scan** to show wireless networks in range, then select the wireless network that you with to repeat (extend its range), and provide the required security for the network. Similar to the Access Point mode, you can also define the **Local IP Settings**. Select **DHCP**, and the Intellinet access point will receive it's IP settings from a DHCP server in your network, most likely that will be your router, and select **Static** if you want to control the IP address and related settings yourself.

STATUS

This section provides various bits and pieces of information about the current status of the Intellinet CPE Wireless Access Point. Depending on the operational mode the device is set to, you will see one of the four possible menus below.



- **WAN**
  If the access point is operating in Router (Gateway) mode, you can see information about the status of the Internet connection on this page, including, but not limited to the WAN IP address and data traffic. Additional information can be found on the WAN page's side bar in your web browser.

- **WISP**
  If the Intellinet CPE Access Point is connected to a wireless ISP, some related information about the WISP connection can be obtained from this status screen. Refer to the help side bar on the WISP information page in your web browser.

- **Repeater**
  If the device is set up as a repeater, you can see information on the current connection status on this page. This can be helpful if you need to trouble shoot a potential problem related to the repeater connection.

- **Access Point**
  This option is available regardless of the operational mode and shows related information to the current wireless function, such as the SSID, channel, security or connected clients.

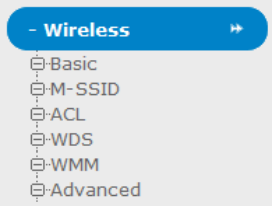
- **LAN**
  This option is available regardless of the operational mode and shows information relevant to the LAN connection status of the Intellinet CPE Access Point, including for example its IP address.

- **DHCP Server**
  The Intellinet CPE Access Point is equipped with an internal DHCP server, which means it can provide IP addresses to connected clients. This screen shows which clients are connected in total, and of those, which have obtained an IP address from the Intellinet CPE Access Point.

- **System**
  Basic system information, including firmware version, hardware version and system uptime.

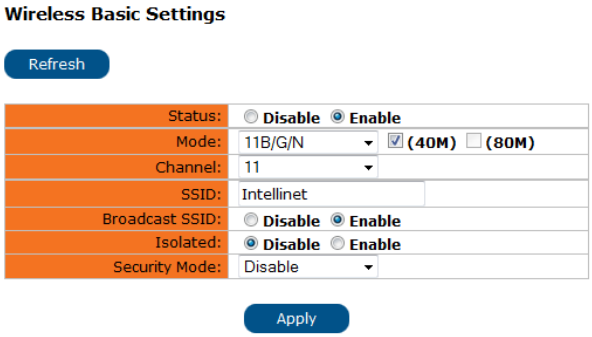
WIRELESS SETTINGS

This menu provides access to all parameters related to the wireless function of the Intellinet CPE Access Point.



BASIC

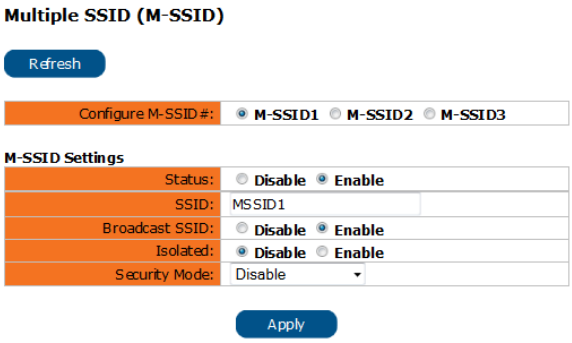
As the name suggests, here you can control the basic settings related to the wireless function. You can define the name of the wireless network (SSID), the channel, security settings, i.e., the wireless password, you can activate wireless client isolation which prevents communication between wireless clients, and you can enable or disable the broadcast of the SSID. For information about the security settings, refer to section Operation Modes – Access Point.



M-SSID

The Intellinet CPE can simultaneously broadcast four different wireless networks (SSIDs). Each wireless network can have its own settings.

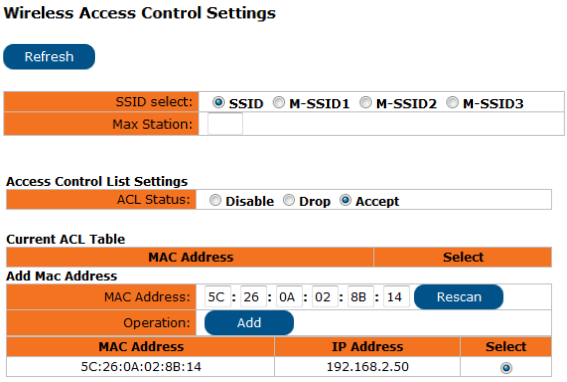
M-SSID Select lets you define, which of the three additional SSIDs you want to configure. Once selected, you can proceed setting up the parameters the same way as you did for the main SSID above under **Basic**.



ACL

ACL standards for access control list. With this feature, you can control who has access to the wireless network, and how many simultaneous users area allowed. All of this can be controlled for each of the four SSIDs independently.

M-SSID Select lets you define, which of the four SSIDs you want to configure. The **Max Station** parameter allows to define an upper connection limit for the particular SSID. This can be helpful if the access point is installed in a busy area and you need to put a cap on the active users to ensure a decent wireless performance for the connected network clients.

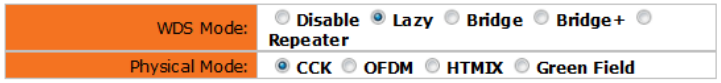

Wireless Access Control Settings
Refresh
SSID select: SSID M-SSID1 M-SSID2 M-SSID3
Max Station:
Access Control List Settings
ACL Status: Disable Drop Accept
Current ACL Table
MAC Address Select
Add Mac Address
MAC Address: 5C : 26 : 0A : 02 : 8B : 14 Rescan
Operation: Add
MAC Address IP Address Select
5C:26:0A:02:8B:14 192.168.2.50

The second feature is the **ACL Status**, which allows (value “Accept”) or disallows (value “Drop”) access based on the MAC address of the wireless network client. Enter the **Mac Address** manually, or click the **Rescan** button to find the MAC address of a connected wireless client automatically, and then click **Add** to add the MAC address to the configuration.

WDS

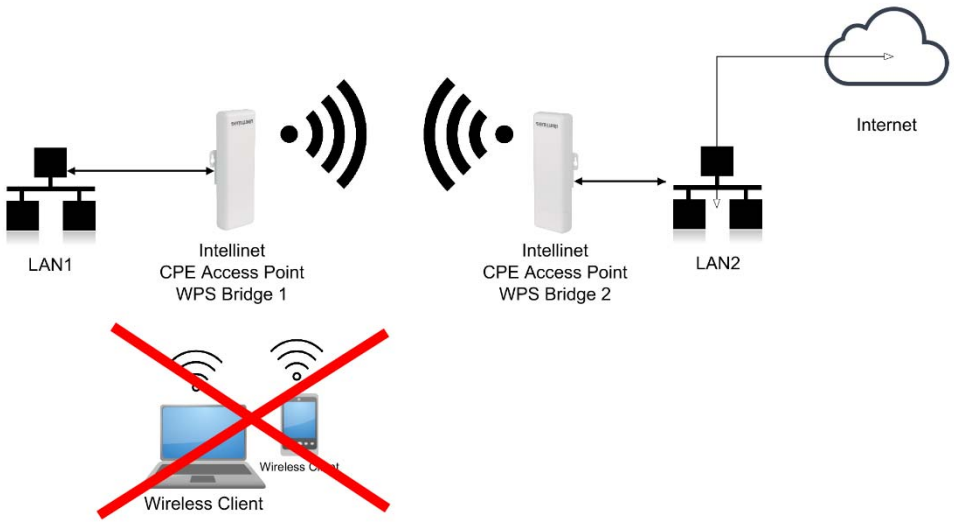
WDS (Wireless Distribution System) is a method of linking two or more wireless access points or wireless routers together, without physically connecting them. WDS is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them, and that saves installation cost.

But WDS isn’t without its problems. Depending on the WDS setup, the performance can suffer greatly, as much as a loss of 50% of transfer speed per hop (access point in WDS mode). If throughput and low latency are important to you, then WDS, as implemented in non-enterprise equipment such as your Intellinet CPE Access Point, isn’t really a good option. WDS also suffers from the problem that only static WPA keys can be used, eliminating one of the key strength of WPA2 encrypted wireless networks. If security is of great importance to you, WDS isn’t the ideal mode to use for your wireless network. WDS setups are also restricted in that only the same equipment can be used in the setup. Even other access points from the same manufacturer, Intellinet included, may not be compatible due to the fact that often different chipsets from different chipset manufacturers are used.

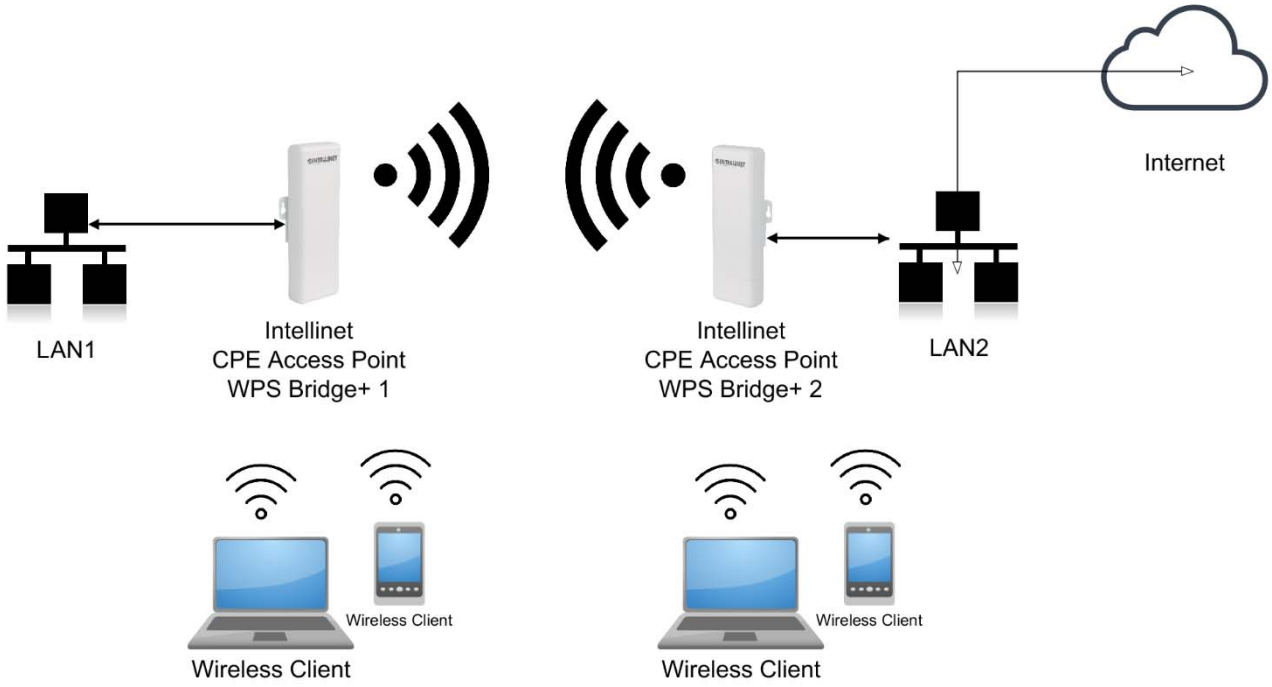


Available modes:
Lazy – In this mode the access point will automatically connect with other WDS devices that use the same SSID, channel, encryption mode, and physical mode. There is no need to manually type in the MAC addresses of the other WDS APs. However, one of the participating access points must be set to Bridge or Bridge+ mode. They can’t all be lazy.

Bridge – This mode can be used to connect two networks together. All WDS bridges must be set to the same channel, SSID, encryption mode and physical mode. Note that the access point in WDS Bridge mode only communicates with other WDS bridges, but not with wireless clients.



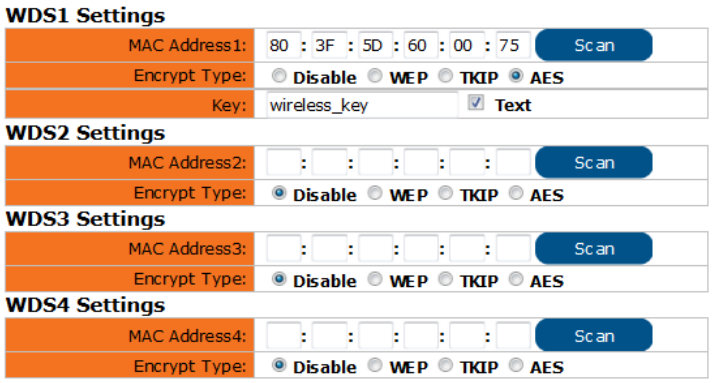
Bridge+ – This mode can be used to connect two networks together. All WDS bridges must be set to the same channel, SSID, encryption mode and physical mode. Unlike Bridge mode, the Bridge+ mode allows the access point to communicate with wireless clients and other WDS bridges at the same time. However, do note that due to the directional antenna characteristics of the Intellinet CPE Access Point, the useable wireless signal is limited to a rather narrow beam. That is good for point to point connections, but when you want to connect wireless clients that are in the vicinity of the access point on all sides, not just in the area of the beam, it is not an ideal solution. In such a situation, the use of an Omni-directional antenna connected to the external antenna connector would be recommended.



Repeater – In this mode, WPS repeaters re-broadcast an existing wireless signal and by doing so extend the range of the wireless network. It works pretty much the same way as the universal repeater mode (see section “Operation Modes”), except the WDS repeater offers some advantages and disadvantages over the standard repeater mode. The advantage is that the WDS repeater creates a transparent wireless repeated network where the connecting devices’ MAC addresses can successfully pass through the network and access to other network clients. As such, the WDS repeater connection is ‘invisible’ to the network clients. It’s as if they were connected via a cable. On the other hand, the universal repeater mode does not provide this transparency, and it is not guaranteed that all clients in the local network can always properly see each other. Not only that, but when using a universal repeater in combination with a wireless hotspot (such as Intellinet’s GuestGate MK II), the login or welcome page may not appear correctly for you as most WiFi hotspot authentication solutions require capturing the MAC address of your tablet, smart phone or laptop which may not successfully pass through the universal repeater. But WDS, as we heard before, has its own share of problems: massive performance penalties, poor compatibility to other hardware and reduced security.

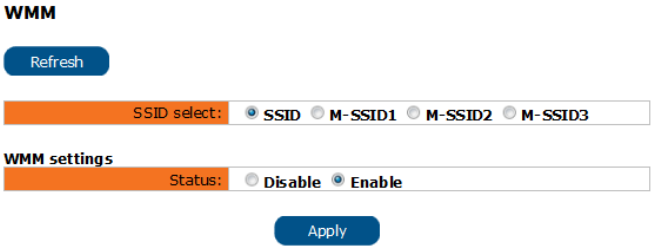
The **Physical Mode** must be set to the same values on all participating WDS access points. You will want to use HTMIX for 11b/g/n mixed mode, and **Green Field** for 802.11n only mode. Select CCK for 802.11b mode and OFDM for 802.11g mode.

You need to provide the MAC addresses of the other WDS APs under **WDS1-4 Settings**, unless you use the lazy mode. Click on Scan to display a list of wireless networks in range and select the network to which you want to create a WDS connection. Select the correct **Encrypt Type** and provide the required **Key**. You can connect to up to 4 different access points in WDS mode.



WMM

Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features for wireless IEEE 802.11 networks. WMM prioritizes traffic according to four access categories (AC for short):

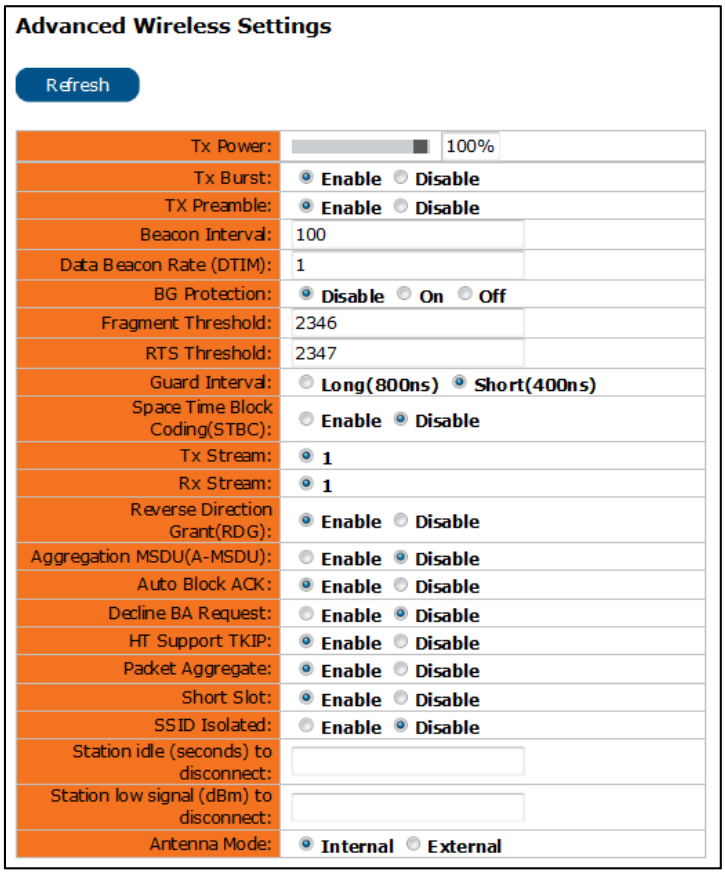


1. Voice
2. Video
3. Best effort
4. Background.

It is suitable for well-defined applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones (VoWLAN). However, it does not provide guaranteed throughput.

As for the Intellinet CPE Access Point, WMM can be disabled or enabled for each of the four SSIDs independently. WMM should be enabled for all SSIDs to ensure the highest possible link speed of 150 Mbps. There is really no reason to disable, unless you are experiencing technical difficulties and want to disable WMM as part of the troubleshooting.

This page provides access to settings and parameters that are best left at their factory default values, unless you have sufficient knowledge about wireless networks. While improper settings cannot cause any harm to the access point, they can have a negative impact on the performance of your wireless network, to the point where you may need to perform a hardware reset on the Intellinet CPE Access Point to get things running smoothly again.


Advanced Wireless Settings
Refresh
Tx Power: 100%
Tx Burst: Enable Disable
TX Preamble: Enable Disable
Beacon Interval: 100
Data Beacon Rate (DTIM): 1
BG Protection: Disable On Off
Fragment Threshold: 2346
RTS Threshold: 2347
Guard Interval: Long(800ns) Short(400ns)
Space Time Block Coding(STBC): Enable Disable
Tx Stream: 1
Rx Stream: 1
Reverse Direction Grant(RDG): Enable Disable
Aggregation MSDU(A-MSDU): Enable Disable
Auto Block ACK: Enable Disable
Decline BA Request: Enable Disable
HT Support TKIP: Enable Disable
Packet Aggregate: Enable Disable
Short Slot: Enable Disable
SSID Isolated: Enable Disable
Station idle (seconds) to disconnect:
Station low signal (dBm) to disconnect:
Antenna Mode: Internal External

TX Power: Controls the strength of the wireless signal.

TX Burst: Tx Burst mode (packet overdrive) is only applicable for IEEE 802.11b/g clients, which means that Tx Bursting does not apply to wireless IEEE 802.11n or IEEE 802.11ac networks.

TX Preamble: Enable or disable the short preamble. If set to **Enable**, the access point will operate with the short preamble settings, and if set to **Disable**, the long preamble is active. Unless you have legacy 802.11b (1 or 2Mbps) clients in your network, there's no need for a long preamble, and you can leave this option enabled.

Beacon Interval: A wireless access points sends out specific data packets containing the SSID, the channel number, and security settings. These packets are called beacons. Any client that wants to join a wireless network listens for these beacon frames, and any wireless client already connected also receives them whenever they are sent out. The beacon interval controls how often the access point broadcasts the beacon frames. Possible values range from 20 to 1000 (ms). The shorter the beacon interval, the more often are the beacon frames sent out. The more often the beacon frames are sent out, the quicker the association and roaming process will be, but it also leads to more network overhead, which then leads to a drop in throughput performance. Increase the beacon interval to reduce the network overhead, but that comes at the expensive of a slightly slower association time, which means it takes just a little bit longer for wireless clients to join the network. The default value is 100.

Data Beacon Rate (DTIM): The DTIM (delivery traffic indication map) rate notifies a wireless client with power-save mode how many beacons until buffered multicast traffic will be broadcast by the access point. The higher the DTIM rate, the longer a client device may sleep and therefore the more power that particular client device may potentially save. You can specify a value between 1 and 255. The default value is 1, which makes the DTIM Interval the same as the Beacon Interval.

BG Protection: B/G Protection, should be set to **On**. The B/G Protection mode ensures that older wireless 802.11b and 802.11g devices will not degrade the performance of the much faster wireless 802.11n network. So, if you have a mix of older and newer wireless stations in the network, it's recommended that you enable the protection mechanism. Only if you know for certain that your network consists only of wireless N clients should you consider disabling this option, as it can increase the performance of your connections ever so slightly.

Fragment Threshold: The fragmentation threshold is used to set the maximum packets size that a client will send. The smaller the maximum sizes the better the reliability of the wireless connection, but the performance is likely to decrease. Possible values range from 256 to the default value of 2346 (bytes). So, then when should you change this value? Only if you need to improve the reliability of a wireless connection where performance is secondary. Usually you do more harm than good if you lower the fragment threshold.

RTS Threshold: RTS (Request to send) packets are sent by wireless clients to access points. The clients essentially ask for permission to send the next data packet. The lower the threshold, the more stable your wireless network, since it essentially asks more often when sending packages. The default value is 2347, and you are well advised to leave this value unchanged.

Guard Interval: This option activates the short guard interval (SGI) when set to 400 ns, which can increase your wireless performance by up to 11%. If your wireless access point is installed in a very crowded network environment with different access points occupy different channels all around you, the slower guard interval of 800 ns will provide better results.

Space Time Block Coding (STBC): STBC is an optional feature in the 802.11n standard is used to achieve the signal to noise ratio on the RF receiver.

Reverse Direction Grant (RDG): Improves the efficiency of a two-way communication. Enabling this is recommended.

Aggregation MSDU (A-MSDU) and Auto Block ACK:
Every frame transmitted by an 802.11 device has a significant amount of overhead, including radio level headers, Media Access Control (MAC) frame fields, interframe spacing, and acknowledgment of transmitted frames. At the highest data rates, this overhead can consume more bandwidth than the payload data frame. To address this issue, the 802.11n standard defines two types of frame aggregation: MAC Service Data Unit (MSDU) aggregation and MAC Protocol Data Unit (MPDU) aggregation. Both types group several data frames into one large frame. Because management information needs to be specified only once per frame, the ratio of payload data to the total volume of data is higher, allowing higher throughput.
MSDU aggregation relies on the fact that most mobile access points and most mobile client protocol stacks use Ethernet as their "native" frame format. It collects Ethernet frames to be transmitted to one or multiple destinations and wraps them in a single 802.11n frame. This is efficient because Ethernet headers are much shorter than 802.11 headers. An A-MSDU contains only MSDUs whose DA and SA parameter values map to the same receiver address (RA) and transmitter address (TA) values, i.e., all the MSDUs are intended to be received by a single receiver, and necessarily they are all transmitted by the same transmitter.
MPDU aggregation also collects Ethernet frames to be transmitted to a single destination, but it wraps each frame in an 802.11n MAC header. Normally this is less efficient than MSDU aggregation, but it may be more efficient in environments with high error rates, because of a mechanism called block acknowledgement. This mechanism allows each of the aggregated data frames to be individually acknowledged or retransmitted if affected by an error.

Decline BA Request: The Block ACK Request (BAR) frame is sent prior to a series of frames that the transmitter would like to be acknowledged. Without a block ACK request, the receiver cannot send a block ACK. With this option you can select to either accept or reject peer-BA-requests.

HT Support TKIP: HT stands for High Throughput and is often used as an abbreviation for IEEE 802.11n. When enabled, this option prevents the use of TKIP data encryption when using 802.11n high-throughput data rates.

Packet Aggregate: Packet aggregation is the process of joining multiple packets together into a single transmission unit, in order to reduce the overhead associated with each transmission.

Short Slot: Short slot time reduces the slot time from 20 microseconds to 9 microseconds. When enabled, it increases the throughput on the 802.11g, 2.4-GHz radio. IEEE 802.11b is not compatible with short slot time.

SSID Isolated: Set to enabled if you want to prevent the different SSIDs from seeing each other. When enabled, traffic on one SSID will not be forwarded to any other SSIDs. Note that unlike wireless client isolation, SSID isolation does not prevent wireless clients that are connected to the same SSID from communicating with each other.

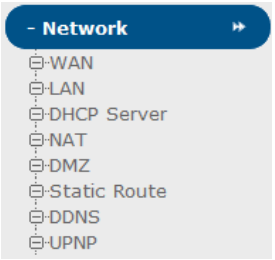
Station Idle to Disconnect (second): Disconnects idel WLAN clients from the network after the specified idle time has elapsed.

Station Low Signal to Disconnect (dBm): If you enable this by entering a dBM value, you can force a wireless client to drop the network, if the signal strength is below the specified threshold value. The idea is that once the client is forced to disconnect, the stations will attempt to re-associate with the best available AP, eliminating the 'sticky node' or ‘sticky client’ problem. Older wireless adapters often exhibit this sticky client behavior where there will associate to an access point and hold on to that association until that signal is gone, despite the fact that all along there were closer access points for them to associate to that would have provided a much stronger connection.

Antenna Mode: if you connect an external antenna to the SMA port of the access point, you need to set it to external, otherwise internal is the right choice.

NETWORK

The Intellinet Wireless CPE Access Points not only provides wireless functionality, but it also allows the clients to connect to and communicate with the local wired network. This section explains the various network configuration options for the different operation modes.



NETWORK SETTINGS IN ROUTER MODE

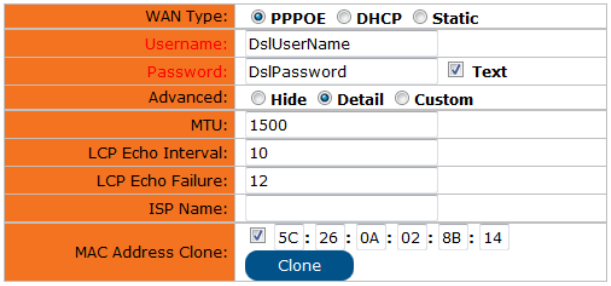
WAN

In router mode, the WAN port of the Intellinet CPE Access Point must be connected to a cable or DSL modem with the WAN port. In addition, you must set up the WAN connection in the device settings. First, you must select the **WAN Type** appropriate for your Internet connection. Available are **PPPoE** (for DSL), **DHCP** (for cable-type Internet) or **Static** (for static IP setups).

PPPoE:

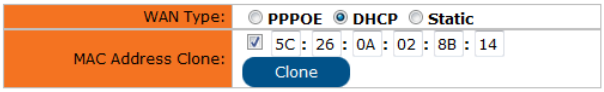
You must provide the username and password for the DSL connection. Additional parameters such as the MTU size, LCP, ISP name and the MAC address may also be required, but that depends on your Internet service provider.

An MTU size of 1500 is considered standard, but smaller MTU values (as low as 1400) can sometimes be required. Again, when in doubt, check with your Internet service provider.


WAN Type: PPPOE DHCP Static
Username: DslUserName
Password: DslPassword Text
Advanced: Hide Detail Custom
MTU: 1500
LCP Echo Interval: 10
LCP Echo Failure: 12
ISP Name:
MAC Address Clone: 5C : 26 : 0A : 02 : 8B : 14
Clone

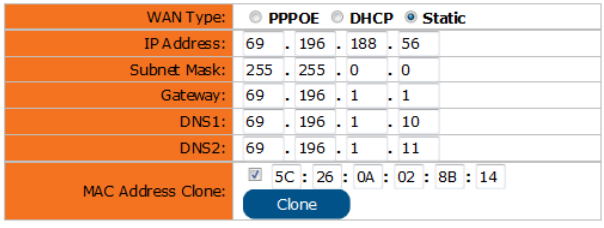
DHCP:

The most common and easiest to set up method. It sometimes requires the MAC address to match the records of the Internet service provider, in which case you can use the MAC Address Clone function.



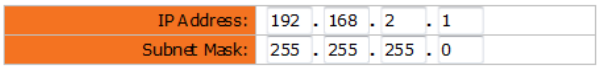
Static:

Should your Internet connection require static IP settings, then you have to enter them on this screen. IP address, subnet mask and DNS1 and mandatory entries. DNS2 is recommended as a backup, and the MAC Address Clone function can be used if the Internet service requires a specific MAC address to be used.


WAN Type: PPPOE DHCP Static
IP Address: 69 . 196 . 188 . 56
Subnet Mask: 255 . 255 . 0 . 0
Gateway: 69 . 196 . 1 . 1
DNS1: 69 . 196 . 1 . 10
DNS2: 69 . 196 . 1 . 11
MAC Address Clone: 5C : 26 : 0A : 02 : 8B : 14
Clone

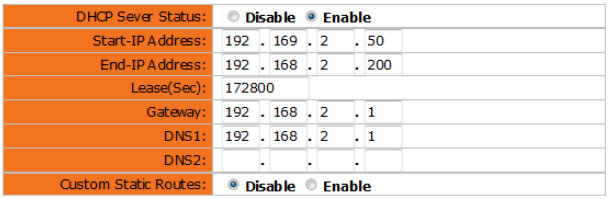
LAN

Here you define the IP address of the Access Point in the local network. The default value is 192.168.2.1 and gives you access to the web UI via http://192.168.2.1. You can make changes to this IP address, e.g., to make the Intellinet access point part of the local network, which may be running on a different subnet.



DHCP Server

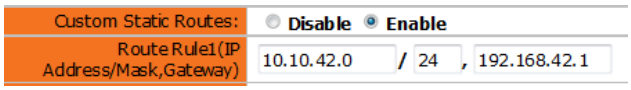
When using the Intellinet CPE Access Point as a router, you will typically want to enable the DHCP server function. Once enabled, the router provides IP address information to the connected clients, just like any ordinary router would do. With that information, clients can access the Internet via the router.


DHCP Sever Status: Disable Enable
Start-IP Address: 192 . 169 . 2 . 50
End-IP Address: 192 . 168 . 2 . 200
Lease(Sec): 172800
Gateway: 192 . 168 . 2 . 1
DNS1: 192 . 168 . 2 . 1
DNS2:
Custom Static Routes: Disable Enable

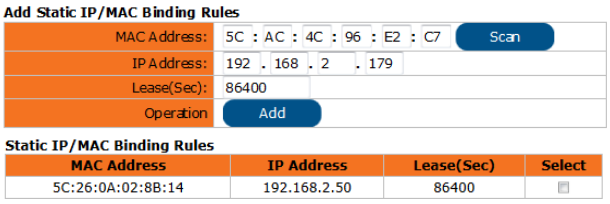
For information about the IP addresses, lease, gateway and DNS, refer to the on-screen help.

Custom Static Routes: Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing protocol to forward traffic. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive.

Example: To route IP traffic destined for the network 10.10.42.0/24 via the next-hop router with the IPv4 address of 192.168.42.1, enter the following information:

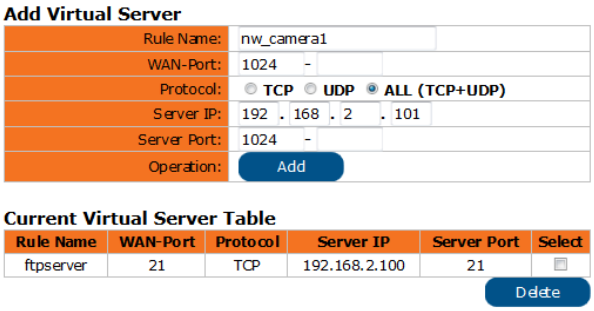


Add Static IP/MAC Binding Rules: In order to ensure that a network client always receives the same IP address from the router, you can have the router assign a static IP address to that client. This can be helpful if you have a local server for which you want to assign a static IP without actually having to configure a static IP address on the local server. To assign a static allocation, type in the MAC address of the client for which you want to create a static DHCP lease, and also type in the IP address and lease time you wish to use. Click **Add** to create the static IP/Mac binding rule.



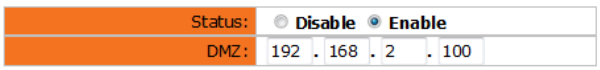
NAT

If you want to make certain local network clients, called servers in this circumstance, accessible from the Internet, you need to create so-called port forwarding rules. Without those rules in place, the router would simply reject any connection attempt made to the service port in question. For example, if you have a local FTP Server that is installed with a static IP address of 192.168.2.100, then you need to create a port forwarding rule for port 21 TCP (Standard FTP) for that IP address. Now if a user from outside your LAN sends a request to the router on port 21, the router will then promptly forward the request to IP address 192.168.2.100. Refer to the on-screen help for additional information.



DMZ

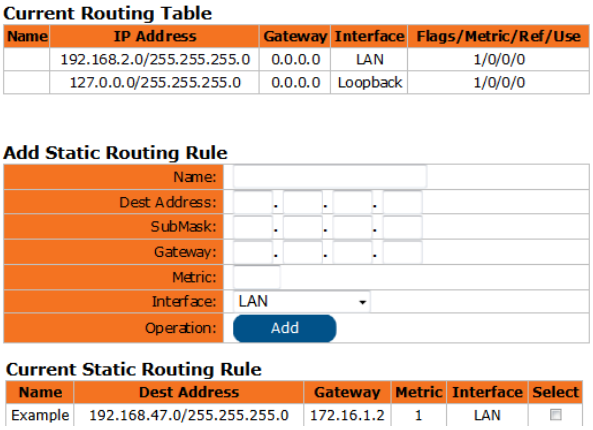
DMZ stands for demilitarized zone. You can activate this option for a single IP address on your local network. Once activated, any traffic sent to your public IP address for any service port will be redirected to the local IP address specified as the DMZ host. If we apply this to our example of FTP server at IP 192.168.2.100, it would mean that not only packets for port 21 are being forwarded to its IP address, but any request on any port. As this completely exposes the local server on IP 192.168.2.100 to traffic on the Internet, that server is at greater risk of being attacked by hackers,



worms, viruses or script kiddies.

Static Route

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing protocol to forward traffic. Setting up static routes requires fundamental understanding of TCP/IP and should only be done by qualified personal. Refer to the on-screen help for additional information.



Current Routing Table

Name	IP Address	Gateway	Interface	Flags/Metric/Ref/Use
	192.168.2.0/255.255.255.0	0.0.0.0	LAN	1/0/0/0
	127.0.0.0/255.255.255.0	0.0.0.0	Loopback	1/0/0/0

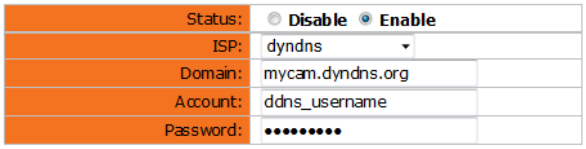
Add Static Routing Rule

Name:	
Dest Address:	. . .
SubMask:	. . .
Gateway:	. . .
Metric:	
Interface:	LAN
Operation:	Add

Current Static Routing Rule

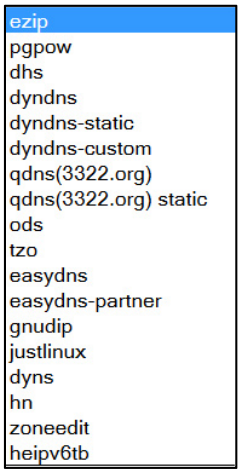
Name	Dest Address	Gateway	Metric	Interface	Select
Example	192.168.47.0/255.255.255.0	172.16.1.2	1	LAN	

DDNS



Status:	Disable Enable
ISP:	dyndns
Domain:	mycam.dyndns.org
Account:	ddns_username
Password:	•••••••••

DDNS (Dynamic DNS) is an IP-to-hostname mapping service for Internet users who don't have a static (fixed) IP address. It will be a problem when a user wants to provide services to other users on the Internet because their IP addresses will vary every time they connect, and they will not be able to know the IP address they're using at any certain time. This router supports the DDNS service of a plethora of service providers. Refer to the on-screen help for additional information.



- ezip
- pgpow
- dhs
- dyndns
- dyndns-static
- dyndns-custom
- qdns(3322.org)
- qdns(3322.org) static
- ods
- tzo
- easydns
- easydns-partner
- gnudip
- justlinux
- dyns
- hn
- zoneedit
- heipv6tb

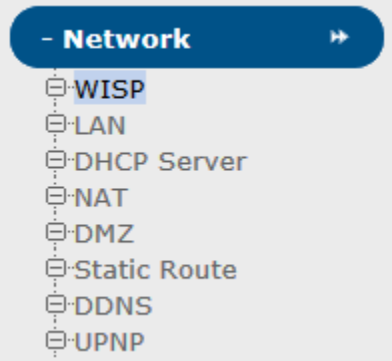
UPNP

Status:	Disable Enable

This function enables network auto-configuration for peer-to-peer communications. With this function, network devices will be able to communicate with other UPnP-enabled devices directly and learn about other devices. Many network devices and applications rely on UPnP function nowadays.

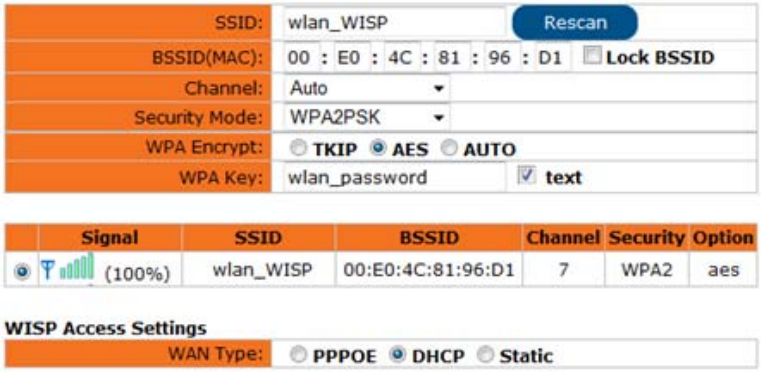
NETWORK SETTINGS IN WISP MODE

When the Intellinet CPE Access Point operates in WISP mode, it connects wirelessly to a 2.4 GHz WiFi signal from a Wireless Internet Service Provider.



All options except for WISP are identical to the Router mode as discussed in the previous section.

Click on **Scan/Rescan** to search for available wireless signals in the area. Select the wireless network ("wlan_ISP" in the example), and the channel, security mode and WLAN Encrypt will be filled out automatically. Type in the password for the wireless network in the field **WPA Key**. Note that this is only required if the WISP signal uses WPA encryption. Should the WISP signal use WEP encryption, the interface presents you with slightly different fields that need to be filled out, namely the WEP key type, key identifier and the actual WEP key fields.

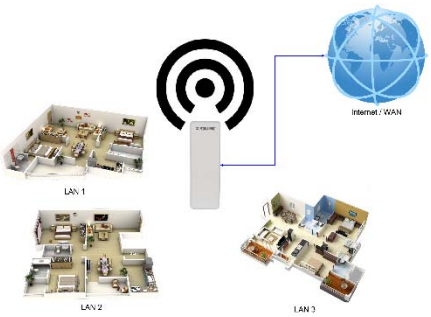

SSID: wlan_WISP Rescan
BSSID(MAC): 00 : E0 : 4C : 81 : 96 : D1 Lock BSSID
Channel: Auto
Security Mode: WPA2PSK
WPA Encrypt: TKIP AES AUTO
WPA Key: wlan_password text
Signal SSID BSSID Channel Security Option
(100%) wlan_WISP 00:E0:4C:81:96:D1 7 WPA2 aes
WISP Access Settings
WAN Type: PPPOE DHCP Static

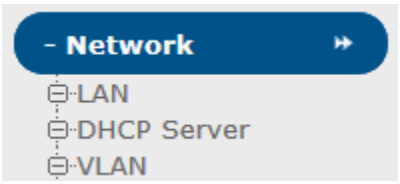
Lock BSSID makes sure that the Intellinet CPE Access Point will always connect to this WISP signal, even if the name of the WISP signal were to ever change.

WISP Access Settings are used to define what type of Internet connection the WISP signal uses. Available choices are **PPPoE** (for DSL), **DHCP** (for cable) and **Static** (IP).

NETWORK SETTINGS IN ACCESS POINT (AP) MODE

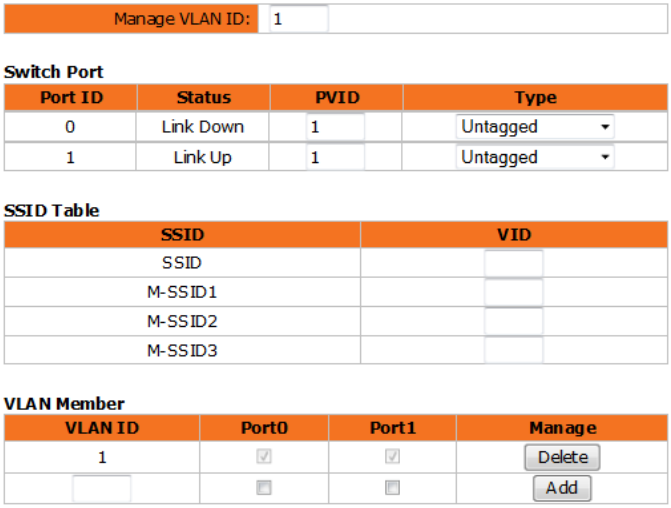
When using the Intellinet CPE as a standard access point (AP), there are not nearly as many settings to configure. LAN and DHCP are even identical to the router mode.





VLAN: The Intellinet CPE Access Point supports tagged VLAN. A VLAN (Virtual Local Area Network) is a method of creating an independent logical network within a physical network. VLAN Tagging is the practice of inserting a VLAN ID into a packet header, which serves as an identifier for which VLAN the packet belongs to. More specifically, switches use the VLAN ID to determine which port or ports to send the packet to.

Manage VLAN ID: Define which VLAN ID is used to manage the access point. Note that if you change this value and click **Apply**, the access point will reboot and after that you will need to have a station that is in that VLAN in order to access the Web admin interface. If you accidentally changed the Management VLAN ID and have lost access to the web admin interface, you will need to perform a hardware reset to restore the factory default settings.



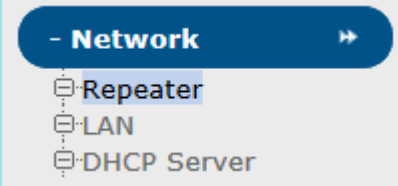
Switch Port: The Intellinet CPE Access Point is equipped with two RJ45 Fast-Ethernet ports. The LAN connector is listed as Port ID 1 and the WAN connector is listed as Port ID 0 – see section "Connectors." For each port you can define the PVID (Port VLAN ID for port-based VLANs) and the tagging status – untagged or tagged.

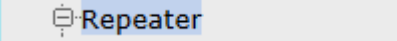
SSID Table: Each of the SSIDs of your Intellinet CPE Access Point can be assigned to a VLAN ID (VID). Leave the VID empty if you want traffic on that SSID not to be tagged.

VLAN Member: Define to which VLANs the physical ports 0 and 1 belong to.

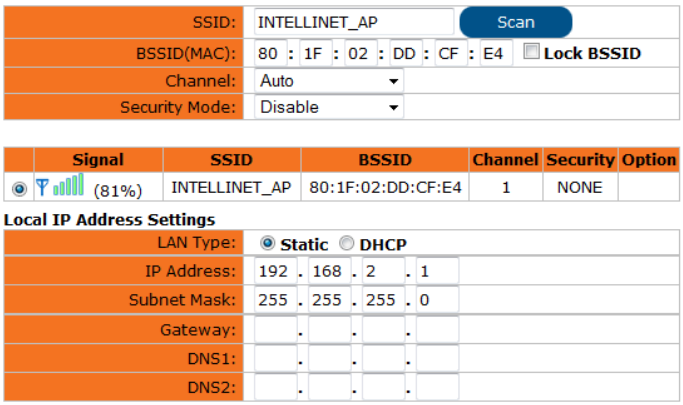
NETWORK SETTINGS IN REPEATER MODE

Repeater mode has the purpose of strengthening an existing wireless signal and extending its range. So it comes as no surprise that the repeater mode is also referred to as range extender mode.



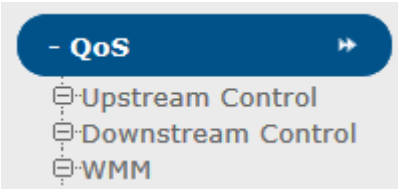


Click **Scan** to show wireless networks in range, then select the wireless network that you with to repeat (extend its range), and provide the required security for the network. You do not need to manually specify the channel or security mode. These values will be automatically filled out based upon which SSID you select.


SSID: INTELLINET_AP Scan
BSSID(MAC): 80 : 1F : 02 : DD : CF : E4 Lock BSSID
Channel: Auto
Security Mode: Disable
Signal SSID BSSID Channel Security Option
(81%) INTELLINET_AP 80:1F:02:DD:CF:E4 1 NONE
Local IP Address Settings
LAN Type: Static DHCP
IP Address: 192 . 168 . 2 . 1
Subnet Mask: 255 . 255 . 255 . 0
Gateway:
DNS1:
DNS2:

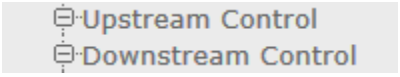
Similar to the Access Point mode, you can also define the **Local IP Settings**. Select **DHCP**, and the Intellinet access point will receive its IP settings from a DHCP server in your network, most likely that will be your router. Select **Static** if you want to control the IP address and related settings yourself. If you want to maintain control over the LAN IP address of the Intellinet CPE Access Point so that you can always quickly access its web configuration interface, using a static IP address might be beneficial – unless you can have your DHCP server assign a static IP address to the Intellinet CPA Access Point.

QOS (IN ROUTER AND WISP MODE)

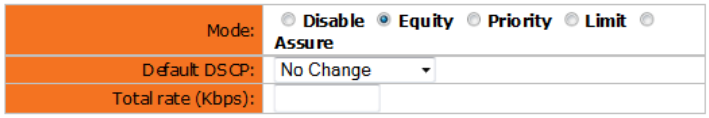


Quality of service (QoS) is the overall performance of computer network, particularly the performance seen by the users of the network. Quality of service is particularly important for the transport of traffic with special requirements. In particular, video or voice over IP applications. QoS, which is also known as traffic shaping, assigns a priority to each device (or service) operating on the network and controls the amount of bandwidth each is allowed to consume based on its role. Without this kind of control, each device would use up as much bandwidth as possible. Proper Quality of Service is advisable if you use your network to play online games, make VoIP such as Skype calls, watch YouTube or stream video for example to Twitch.

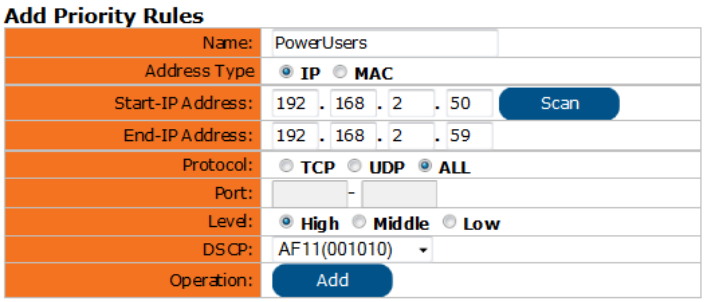
Configuring QoS can be quite complex, and the Intellinet CPE Access Point allows a very detailed control over the data and how it is prioritized indeed. Setting this up incorrectly can cause more harm than good, and because of that it is highly recommended that you are familiar with QoS and its related terms such as DSCP, etc.



This is where things get trickier. Upstream describes all data traffic that you send from your local network to the Internet, for instance, traffic from your PC to your Twitch or YouTube live broadcast. Downstream is the opposite. If you watch a video on YouTube, data is sent from the Internet to your local network, and that is considered download or downstream.

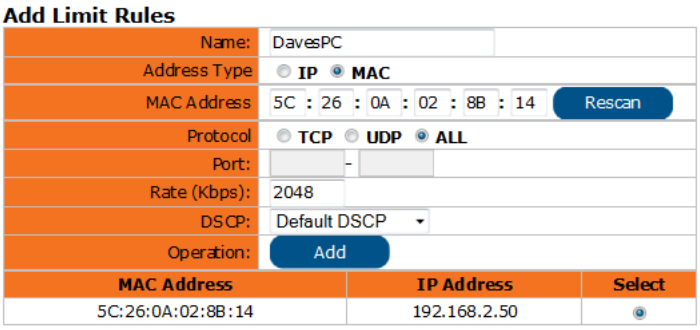


Mode - Equity: The access point will try its best to distribute the available bandwidth evenly and fairly between the available network clients. No one client will be especially limited or given any special treatment over the other. This mode is not as effective as Priority, Limit or Assure.



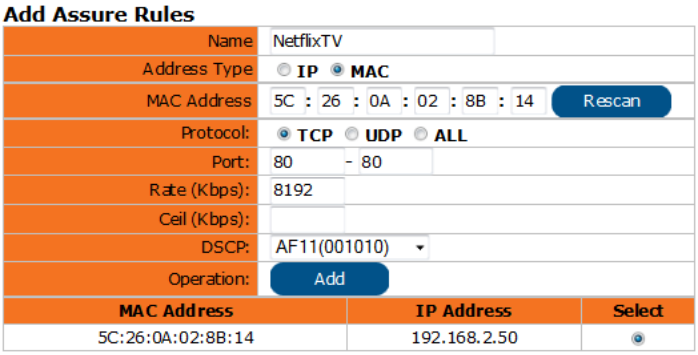
Mode - Priority: When selected, you can assign network clients one of three possible priorities. This allows you to quickly categorize network clients, for example guests, normal users and power users. The example on the right shows an example on how to create a rule for 10 computers (IP 192.168.2.50 – 192.168.2.59) which have high priority **Level** with **DSCP** set to AF11.
You can identify computers based on their IP addresses (as shown), or based on their **MAC** address. Furthermore, you can limit the rule to only affect traffic for a certain **Protocol** (TCP or UDP) and **Port**.

Mode - Limit: With this mode you have the ability to limit the bandwidth available a certain network client or a group of network clients. The idea behind this is to provide a cap for the available upload or download bandwidth.

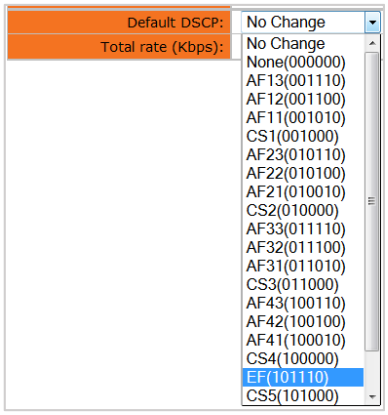


The example shows how we create a rule that limits the available bandwidth for a PC (presumably Dave's) with the MAC address 5C:26:0A:02:8B:14 to 2048 Kbps or 2 Mbps. The DSP value is kept at default (= best effort), which makes sense in this type of scenario.

Mode - Assure: With this mode you have the ability to guarantee bandwidth to an individual client, or a group of clients. The example on the right shows how to add a Netflix video streaming device and make sure it has sufficient bandwidth available to stream in 1080p resolution. Netflix uses the TCP **Protocol** on **Port** 80. As for the bandwidth, 5 Mbps are typically sufficient, but to be on the safe side, we reserve a little bit more and set the **Rate (kbps)** to 8192 (= 8 Mbps). The Ceil (kbps) can be used to limit the maximum bandwidth available to the device, but we don't want to do that in this case. We also set the **DSCP** to AF11 to boost the traffic priority.

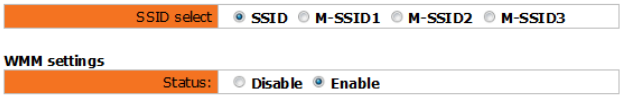


Default DSCP: DSCP stands for differentiated services code point. It is a field in an IP packet that enables different levels of service to be assigned to network traffic. The DSCP value can tell your ISP how to handle your traffic, but most ISPs will ignore DSCP markings as they leave your network and enter theirs, and for good reasons: Net Neutrality. If ISPS would respect and act upon these headers, they would quickly become meaningless since everybody would code their traffic for the highest priority (Expedited Forwarding "EF"). In reality DSCP can really only affect the data traffic inside your network, and how the router prioritizes it. Combine a DSCP value of **EF** with **Priority** mode for example, and the router will give the highest priority to that traffic up to the point where it leaves your network. See Appendix C for information about the DSCP values.



Total rate (kbps): Define how much total bandwidth (upstream plus downstream) in kbps is available. This parameter needs to be provided in Assure mode.

WMM

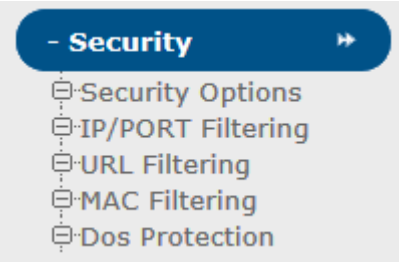


One feature of QoS does not require any configuration. It's called WMM, which standards for WiFi Multimedia. WMM prioritizes network traffic in four categories:

1. Voice
2. Video
3. Best effort (this is the majority of traffic from applications other than video and voice)
4. Background jobs such as printing, file downloads and other non-latency sensitive applications.

Simply by activating WMM for the SSIDs of the Intellinet CPE Access Point you can already achieve a noticeable improvement of the quality of service.

SECURITY (IN ROUTER AND WISP MODE)



The Intellinet CPE Access Point is equipped with a Firewall that protects local network users from hacker attacks from the Internet whenever router or WISP mode is used. IN these modes there are two layers of security. First, NAT itself. A NAT router by design provides protection for local network users in that it will not forward a request made from the Internet to a specific service port, unless that request is a response to an inquiry made from a local client. Second, the Intellinet CPE Access Point provides additional features such as IP, Port or MAC address filtering, which allow a more direct control of who can access the device and services, and who cannot.

Security Options

Default Rules: Specify the default behavior. Everything that isn't covered by any of the security rules is either being dropped or accepted (default) – depending on how you set this value up. Accept is the correct choice in the vast majority of the cases.

Default Rules:	Accept / Drop
IP/PORT Filtering:	Disable / Enable
MAC Filtering:	Disable / Enable
URL Filtering:	Disable / Enable
DoS Protection:	Disable / Enable
Remote Ping Access:	Disable / Enable
Remote WEB Access:	Disable / Enable
Remote Telnet Access:	Disable / Enable
Remote SNMP Access:	Disable / Enable
Remote FTP Access:	Disable / Enable
Remote Samba Access:	Disable / Enable

IP/Port Filtering: You can create specific rules for IP addresses and ports.

MAC Filtering: You can create specific rules for individual MAC addreses.

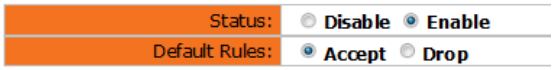
URL Filtering: Block or allow access to web pages.

DoS Protection: Provides additional security against DoS (Dial of Service) attacks.

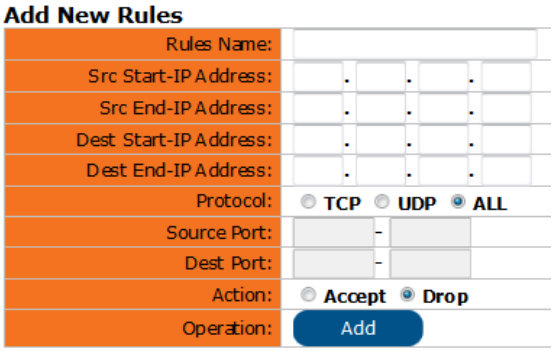
There are several parameters that can be activated or deactivated. Note that the default values are such, that remote access to local services is prohibited – that includes **Ping, WEB, Telnet, SNMP, FTP** and **Samba access**. Unless you have good reasons, it's best to leave these options set to **Disable**.

IP/PORT FILTER:

With this screen you can create rules for specific IP addresses, protocols and TCP/UDP ports. You can either grant or deny access.



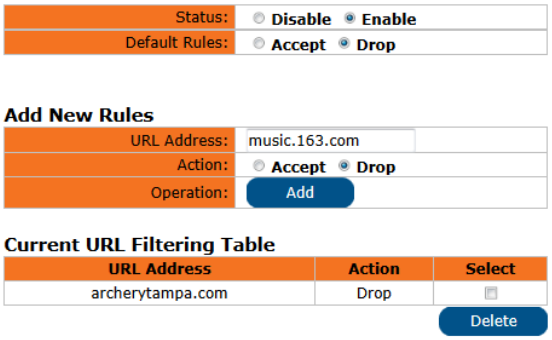
Status: Enable or disable this filter.
Default Rules: Default behavior for any packet not matching any of the defined rules (default = accept).



Rules Name: Provide an easily reconizeable name for the rule.
Src Start-IP-Address: Local IP address affected by the rule.
Src End-IP-Address: If the rule is for a range of IP addresses, you need to specify a start and end address.
Dest Start-IP-Address: Destination IP address affected by the rule.
Dest End-IP-Address: If the rule is for a range of IP addresses, you need to specify a start and end address.
Protocol: Define whether the rule applies to TCP, UDP or both types of connections.
Source and Dest Port: If the rule is to only apply to certain ports, define them here.
Action: Define whether to allow (Accept) or disallow (Drop) any packet that matches this rule.

URL FILTERING:

With this function you can limit access to individual Web pages.

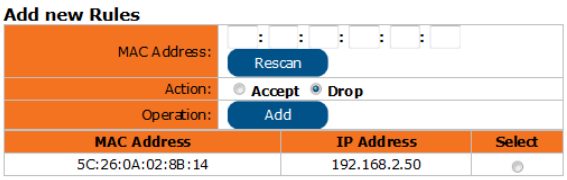


Status: Enable or disable this filter.
Default Rules: Default behavior for any packet not matching any of the defined rules (default = accept).

URL Address: Type in the URL of the site you wish to block or grant access to.
Action: Define whether access to this URL should be allowed or disallowed.

MAC FILTERING:

A media access control address (MAC address) is a unique identifier assigned to network interfaces such as wired or wireless adapters. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and WiFi. This screen lets you create rules for specific MAC addresses. You can either grant or deny access based on the MAC address.



MAC Address: Manually type in the MAC address, or use the **Scan** button to display a list of all connected network clients and then select the one you wish to create the rule.
Action: Define whether to allow (Accept) or disallow (Drop) any packet that matches this rule.

DOS PROTECTION:

In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. The Intellinet CPE Access Point allows you to enable additional barriers against these kinds of attacks. As this function requires a more detailed inspection of the data packets, it can have a negative impact on the overall performance of the wireless network.

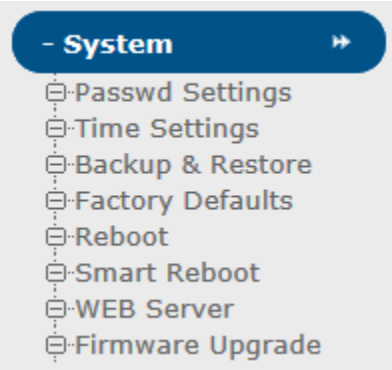
Dos Table

L2TP Filtering:	Disable Enable
PPTP Filtering:	Disable Enable
Port Scan Filtering:	Disable Enable
Netbios Filtering:	Disable Enable
ICMP Send Filtering:	Disable Enable
IP Spoofing Filtering:	Disable Enable
ICMP Flood Filtering:	Disable Enable
UDP Flood Filtering:	Disable Enable
TCP SYN Flood Filtering:	Disable Enable
Ping Death Filtering:	Disable Enable
Land Attach:	Disable Enable
TCP NULL Attach:	Disable Enable
Short Packet Attach:	Disable Enable

For maximum security you may enable all of these options.

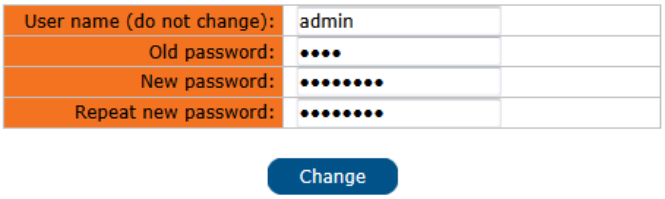
SYSTEM

The Intellinet CPE Access offers several system-related functions, which are discussed in this section. Here you can reboot the device, upgrade the firmware, backup and restore the configuration, and more.



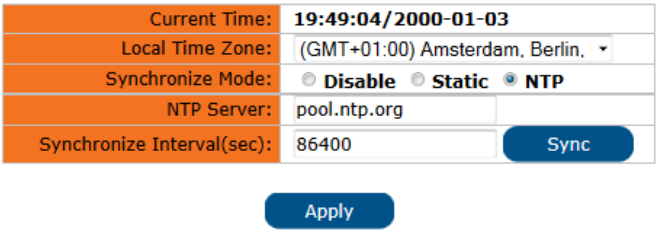
PASSWORD SETTINGS

The default password for accessing the web administrator interface is **1234**. In this menu you can change that password. Changing this password after the initial installation is recommended to prevent unauthorized access to the configuration pages of the Intellinet CPE Access Point.



TIME SETTINGS

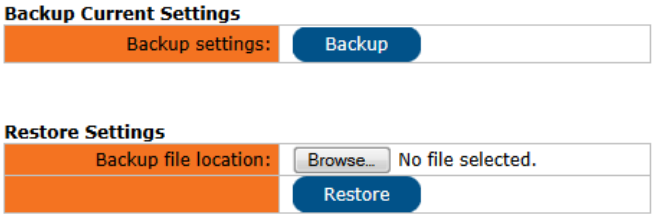
With this screen you can set up the internal time of the Intellinet CPE Access Point. Define the **Local Time Zone**, the **Synchronize Mode**, the **NTP Server** and the **Synchronize Interval**.



If the Access Point is connected to the Internet, you can use the mode NTP. The default NTP server is pool.ntp.org, and it typically works just fine. You can, however, change the NTP server address to something else. If you select static, you must provide the time manually. If you do, be aware that the time will slowly but surely become out of sync with the actual time.

BACKUP & RESTORE

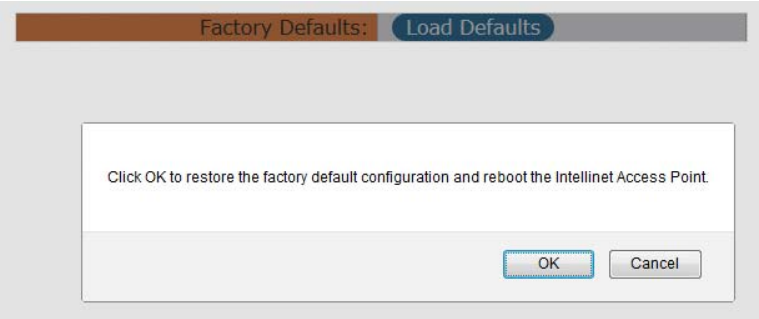
The Backup & Restore option allows you to save a file containing all your access point's configuration settings, like IP address, SSID and security settings, etc. to a file on your computer's HDD. This file can then be used to restore the settings if the access point is reset to the factory default settings.



Backup: Click this button to save the current configuration to your computer's HDD and USB stick.
Restore: Click **Browse**, select the configuration file that you previously saved, and then click **Restore** to re-load the configuration.

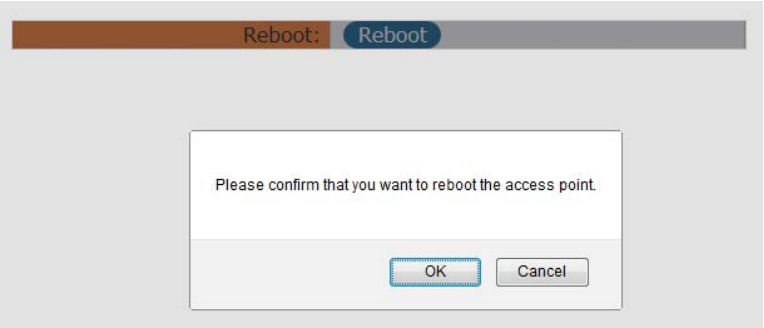
FACTORY DEFAULTS

With this function you can restore the factory default configuration of the Intellinet CPE Access Point. All of your custom configuration settings will be lost when the reset is performed. Click on the **Load Defaults** button to begin the process and confirm your decision by clicking on **OK**.

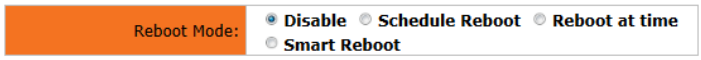

Factory Defaults:
Load Defaults
Click OK to restore the factory default configuration and reboot the Intellinet Access Point.
OK
Cancel

REBOOT

Restart the access point from time to time to free up system resources, or in case the device does not perform properly anymore. Click on **Reboot** to begin the process and confirm your decision by clicking on **OK**.



SMART REBOOT

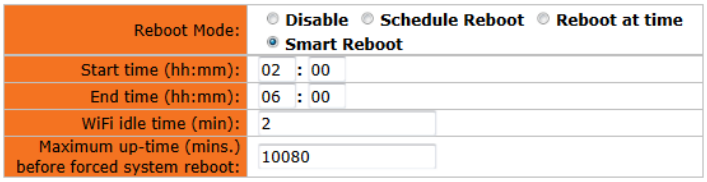


In addition to the manual reboot option (see above), there is another method: The Smart Reboot. What is it for, and how can it be used?
This wireless Access Point, like any other computer, has a finite amount of system resources. Over time, free resources will become less and less, and eventually, the system stability can be compromised. A reboot frees up these system resources and allows continued use of the device.

Scheduled Reboot: When the system reaches a specified running time, the system will reboot automatically. The device will do this reboot, regardless of whether or not any devices are connected. So do keep in mind that you potentially disconnect your wireless users.

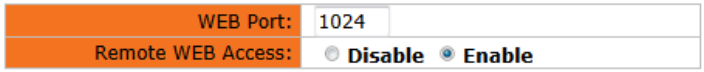
Reboot at time: In this mode the device will reboot once every 24 hours. You can specify at what time this should happen. Ideally, you will want to choose a time that has little to no active connections going on, e.g., in the middle of the night, because existing wireless connections will be ignored and existing sessions will be interrupted.

Smart Reboot: This mode works similar to **Reboot at time**, with the exception that the Intellinet CPE Access Point will try to keep the interruption to the network at an absolute minimum. The way this works is as follows: You specify a time interval in which the access point will try to perform the restart. You also specify the **WiFi idle time**, which specifies how many minutes of no WLAN traffic have to pass before the smart reboot can occur. Finally you can specify how long the Intellinet CPE Access Point will wait, before forcefully restarting without any regard for active connections, by providing a **Maximum up-time (mins.).** For example, if you want to force a reboot at least once per week, you type in 10080 as the maximum up-time (10080 minutes = 7 days).



WEB SERVER

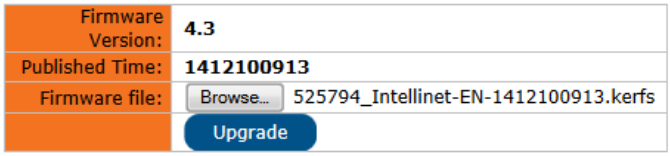
The web administrator configuration interface is accessible like any other web page. By default you can access it by going to http://192.168.2.1 with your Web browser. Each standard HTTP request is made to port 80, unless you specify otherwise. This means that http://192.168.2.1 is the same as http://192.168.2.1:80. If you want to change the port, for example because you want to be able to remotely access the web administrator configuration interface but port 80 is already in use, then you can change the **WEB Port** to something else. In our example the port is changed to the value 1024 and the new URL to access the web administrator configuration interface is http://192.168.2.:1024.



Remote WEB Access: Enable or disable remote WEB server access. If you need to configure the device from outside your LAN, this option should be enabled. In addition, you will need to add the **WEB Port** to your router's port forwarding table and set up the Intellinet CPE Access Point as an internal server.

FIRMWARE UPGRADE

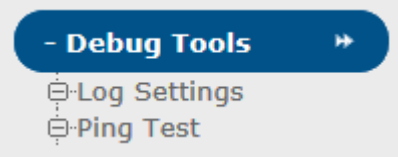
From time to time there might be a new firmware version available for the Intellinet CPE Access Point. A new firmware version can be released to add new features or to fix bugs that have been discovered. A new firmware would be posted on the Intellinet web site (intellinetnetwork.com). In order to upgrade the firmware, the following steps have to be performed:



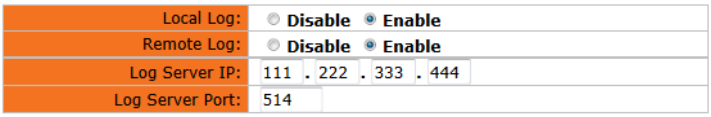
1. Download the new firmware from Intellinetnetwork.com. Search for '525794' to get to the product detail page where the download would be located. Uncompress the ZIP file once the download is completed.
2. Connect to the Intellinet CPE Access Point web administrator configuration interface and open the Firmware Upgrade menu. Note: Be sure to connect to the Access Point via the wired network.
3. Click on Browse to select the firmware you have previously downloaded.
4. Click on Upgrade to begin the process and confirm your decision by clicking on OK.

DEBUG TOOLS

In this section you can find information about two additional features of the Intellinet CPE Access Point.



LOG SETTINGS



The access point generates run-time messages (warnings, errors, etc.) and can provide them for later review in a log. This can either be a **Local Log**, or a **Remote log** utilizing the syslog protocol. **Syslog** is a widely used standard for message logging. It permits separation of the software that generates messages, such as the Intellinet CPE Access Point, and the system that stores them, for example the remote syslog server. If you want to utilize a remote server, then you need to activate the **Remote Log** option and provide the **Log Server IP**. The default syslog **Log Server Port** is 514. You can make changes to the port as needed.

PING TEST

The Intellinet CPE Access Point has the ability to ping other network devices. This can be a useful function if you connect to the access point remotely, but want to verify that a certain client is available on the local network, in which the access point it installed. Simply type in the **IP Address** of the client and click on **Test**.

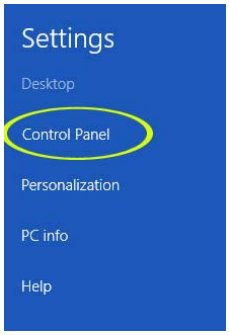
APPENDIX A: CHANGING THE IP ADDRESS OF A NETWORK ADAPTER

The Intellinet CPE Access Point operates on the IP address 192.168.2.1. For your computer to access the administrator configuration interface, the IP address of the network adapter in your computer has to be in the same range; e.g., 192.168.2.50. Refer to the instructions that came with your computer for information on how to change the IP address on the network adapter in your computer for any operating system that is not explained in this user manual.

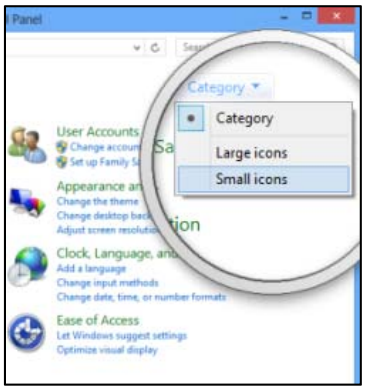
WINDOWS 8

1. If you are using a PC, move the mouse cursor to the bottom or top right corner of the screen and select the cog icon for Settings. If you are using a tablet, swipe left from the right side of the screen and select Settings.

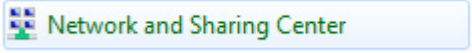
2. Click “Control Panel.”



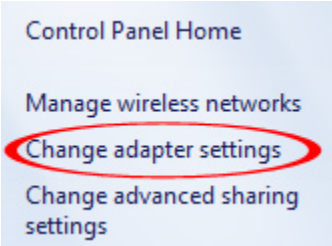
3. Select “Small icons.”



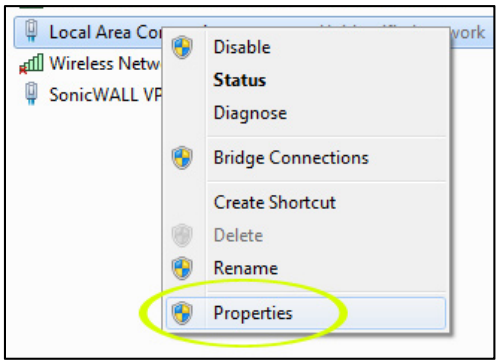
4. Open “Network and Sharing Center.”



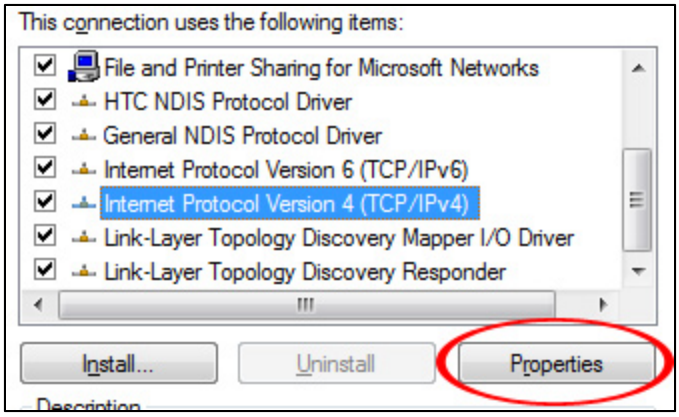
5. Click “Change adapter settings.”



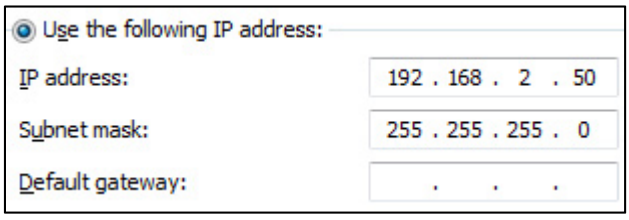
6. Right-click your network adapter and select “Properties.”



7. Select “Internet Protocol Version 4” from the list and click “Properties.”


This connection uses the following items:
File and Printer Sharing for Microsoft Networks
HTC NDIS Protocol Driver
General NDIS Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties

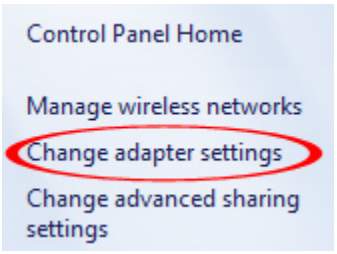
8. Enter the information as shown below, then click “OK” to save the settings.



WINDOWS 7:

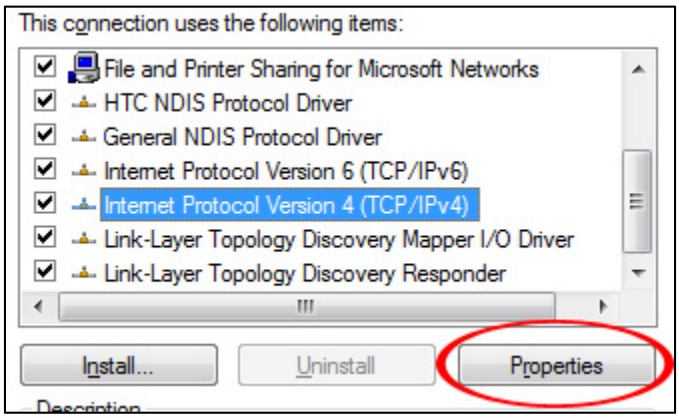
1. Open the Network and Sharing Center.

2. Click on “Change adapter settings.”

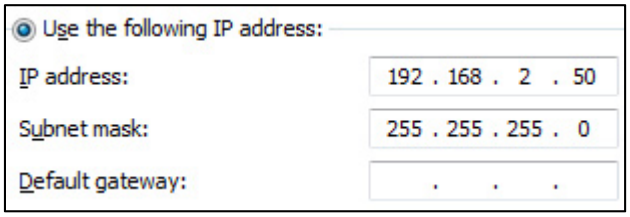


3. Right-click your network adapter and select “Properties.”

4. Select “Internet Protocol Version 4” from the list and click “Properties.”


This connection uses the following items:
File and Printer Sharing for Microsoft Networks
HTC NDIS Protocol Driver
General NDIS Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties

5. Enter the information as shown below, then click “OK” to save the settings.

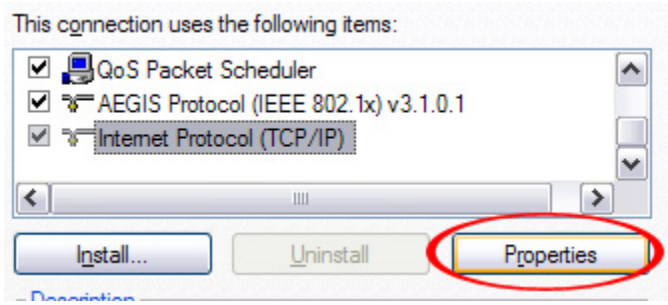


WINDOWS XP:

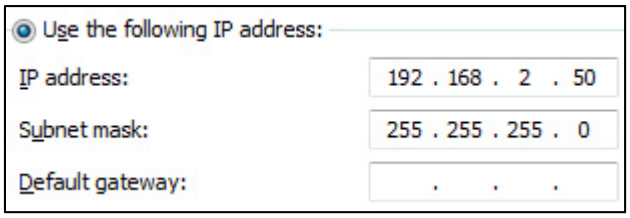
1. Double-click the “Network Connections” icon in the control panel.

2. Right-click the connection (e.g., Local Area Connection) and select “Properties.”

3. Select “Internet Protocol (TCP/IP)” from the list and click “Properties.”



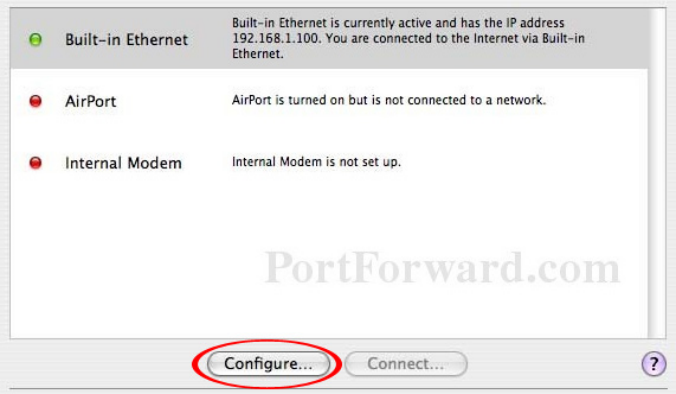
4. Enter the information as shown below, then click “OK” to save the settings.



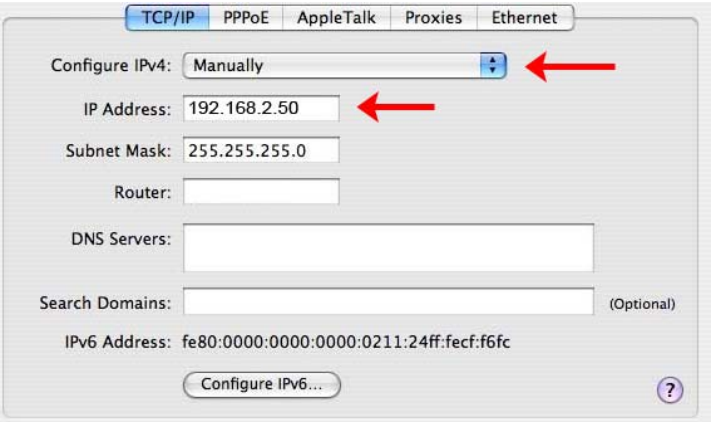
1. Open the System Preferences page.

2. In the Internet & Network section, click the Network icon.

3. Select either Built-in Ethernet or AirPort, depending on how you connect to the wireless range extender, then click "Configure… ."


Built-in Ethernet
Built-in Ethernet is currently active and has the IP address 192.168.1.100. You are connected to the Internet via Built-in Ethernet.
AirPort
AirPort is turned on but is not connected to a network.
Internal Modem
Internal Modem is not set up.
PortForward.com
Configure...
Connect...

4. Set the value for Configure IPv4 to "Manually" and enter 192.168.2.50 in the IP Address field. Click "Apply Now" (not shown in screen shot) to save the settings.



Symptom	How to address
The Power LED is not lit.	Make sure that the power adapter is either properly inserted into the power connector on the PoE injector or the access point itself. If you use the PoE injector, be sure that you use an 8-pin network cable between the PoE injector and the access point's LAN port. A 4-pin cable won't work. Also, if you use the PoE injector, be sure that the Power LED on the injector is lit, and that you have connected the port labeled as "POE" with a network cable to the LAN port on the access point. In addition, check and make sure that the power outlet provides power.
The LAN LED does not light up.	Check the network connection between the access point's LAN port and the Ethernet port of the device you're connecting. The network cable must be inserted properly and the Ethernet device must be turned on. Try using a different network cable, if available.
The WAN LED does not light up.	Check the network connection between the access point's WAN port and the Ethernet port of the modem you're connecting to. The network cable must be inserted properly and the Ethernet device must be turned on. Try using a different network cable, if available.
The WLAN LED is not lit.	The WLAN LED should always be light, whether a wireless connection has been established or not. It essentially indicates that the wireless module has started successfully. If the LED is off, it means that the wireless function has been disabled in the basic wireless settings. If the wireless function is enabled in the wireless setting, but the LED is off and you cannot connect to any wireless network, the access point needs to be replaced through your dealer (place of purchase). If the LED is off yet you have a working wireless connection, the LED may simply have failed.
The hardware reset is not working.	The reset button needs to be pressed firmly for 10 seconds while the wireless range extender is powered on. If it still does not work, the reset button could be malfunctioning.

APPENDIX C: DSCP VALUE TABLE

DSCP Name	DS Field Value		IP Precedence
	Binary	Decimal	
AF11	001 010	10	001 - Priority
AF12	001 100	12	001 - Priority
AF13	001 110	14	001 - Priority
AF21	010 010	18	001 - Immediate
AF22	010 100	20	001 - Immediate
AF23	010 110	22	001 - Immediate
AF31	011 010	26	011 - Flash
AF32	011 100	28	011 - Flash
AF33	011 110	30	011 - Flash
AF41	100 010	34	100 - Flash Override
AF42	100 100	36	100 - Flash Override
AF43	100 110	38	100 - Flash Override
None / Best Effort	000 000	0	0000 - Routine
CS1	001 000	8	1
CS2	010 000	16	2
CS3	011 000	24	3
CS4	100 000	32	4
CS5	101 000	40	5
CS6	110 000	48	6
CS7	111 000	56	7
EF (High Priority)	101 110	46	101 - Critical

APPENDIX D: WARRANTY INFORMATION

Deutsch Garantieinformationen finden Sie hier unter intellinetnetwork.com/warranty.

English For warranty information, go to intellinetnetwork.com/warranty.

Español Si desea obtener información sobre la garantía, visite intellinetnetwork.com/warranty.

Français Pour consulter les informations sur la garantie, rendezvous à l'adresse intellinetnetwork.com/warranty.

Italiano Per informazioni sulla garanzia, accedere a intellinetnetwork.com/warranty.

Polski Informacje dotyczące gwarancji znajdują się na stronie intellinetnetwork.com/warranty.

México Póliza de Garantía Intellinet — Datos del importador y responsable ante el consumidor IC Intracom México, S.A.P.I. de C.V. • Av. Interceptor Poniente # 73, Col. Parque Industrial La Joya, Cuautitlan Izcalli, Estado de México, C.P. 54730, México. • Tel. (55)1500-4500

La presente garantía cubre los siguientes productos contra cualquier defecto de fabricación en sus materiales y mano de obra.
A. Garantizamos cámaras IP y productos con partes móviles por 3 años.
B. Garantizamos los demás productos por 5 años (productos sin partes móviles), bajo las siguientes condiciones:
1. Todos los productos a que se refiere esta garantía, ampara su cambio físico, sin ningún cargo para el consumidor.
2. El comercializador no tiene talleres de servicio, debido a que los productos que se garantizan no cuentan con reparaciones, ni refacciones, ya que su garantía es de cambio físico.
3. La garantía cubre exclusivamente aquellas partes, equipos o sub-ensambles que hayan sido instaladas de fábrica y no incluye en ningún caso el equipo adicional o cualesquiera que hayan sido adicionados al mismo por el usuario o distribuidor.

Para hacer efectiva esta garantía bastará con presentar el producto al distribuidor en el domicilio donde ue adquirido o en el domicilio de IC Intracom México, S.A.P.I. de C.V., junto con los accesorios contenidos n su empaque, acompañado de su póliza debidamente llenada y sellada por la casa vendedora indispensable el sello y fecha de compra) donde lo adquirió, o bien, la factura o ticket de compra original donde se mencione claramente el modelo, numero de serie (cuando aplique) y fecha de adquisición. Esta garantía no es válida en los siguientes casos: Si el producto se hubiese tilizado en condiciones distintas a las normales; si el producto no ha sido operado conforme a los instructivos de uso; o si el producto ha sido alterado o tratado de ser reparado por el consumidor o terceras personas.

intellinetnetwork.com

© IC Intracom. All rights reserved.
Intellinet is a trademark of IC Intracom, registered in the U.S. and other countries.